Table of Contents

Akuvox Tool > Product

Akuvox
Open A Smart World

WWW.AKUVOX.COM

AKUVOX SDMC

Administrator Guide

Version: 1.0 | Date: Nov.2021

About This Manual

Thank you for reading this manual. This manual is intended for the administrators who need to properly manage the SDMC (SIP Device Management Center) for integrated management and control that incorporates the all-in-one management of the personnel (residents, property manager), network setting, Intercom, message, device, access control configuration, authentication method, logs, lift control, monitoring etc. This manual applies to SDMS with the software version 6.0.0.2. Please visit consult our technical support for any new information or the latest software version.

Introduction of Icons and Symbols

Warning:

- **Always abide by this information in order to prevent the persons from injury.**

Caution:

- **Always abide by this information in order to prevent damages to the device.**

Note:

- **Informative information and advice for the efficient use of the device.**

Related Documentation

You are advised to refer to the related documents for more technical information via the link below:

https://knowledge.akuvox.com

1.SDMC Overview

SDMC (SIP Device Management Center) is generally installed in the community management center. The software serves as a LAN-based on-premise platform designed to manage the personnel, devices, access control, intercom, alarm, message, lift control, video monitoring etc at one stop.

Users using SDMC will be able to:

- To achieve the data synchronization between the SDMC and device.
- To manage the residents, property staff and access control with various types of authentication method.
- To manage the deployment of device on the node basis for residents etc.
- To Make IP/SIP call the intercom devices, and monitor community-wide surroundings for the security purpose.
- To manage various types of logs.

.

- To manage and deal with alarm.
- To manage messaging and Ad Pushing.
- To import and export system data and database for the convenience of data sharing and system configuration.
- To manage the lift control.

2.SDMC Installation

2.1. Installation Requirements

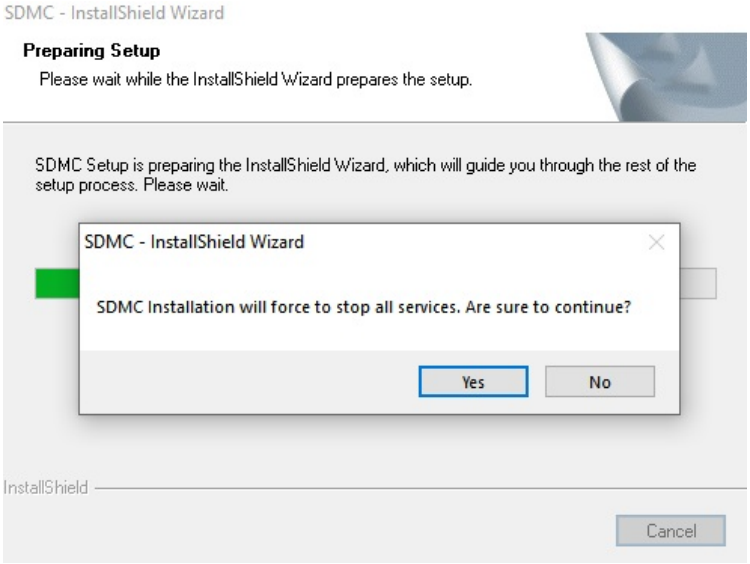
Prior to the installation of the SDMC software, you are required to make sure that the following installation requirements are met:

- Windows 7 operating system or above.
- No SDMC and SDMC software is installed on your personal computer or on other personal computers in the same network.
- The Firewall on your computer is turned off.

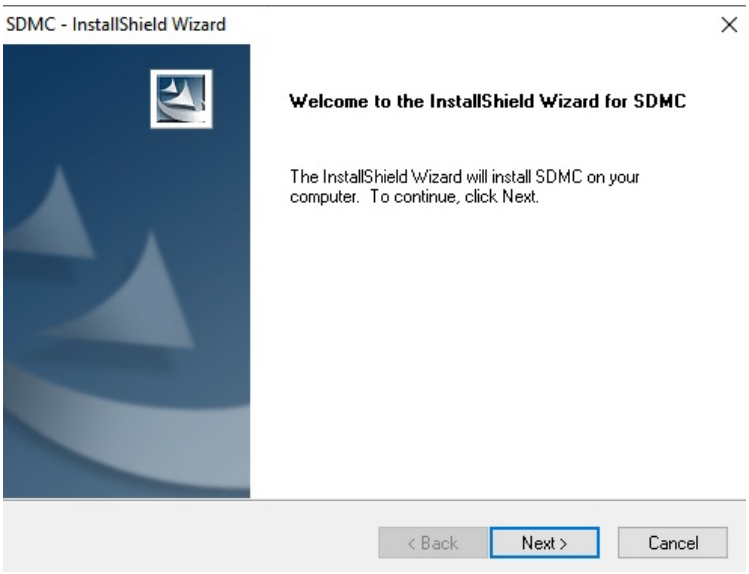
2.2. Install SDMC

Steps to install SDMC[1].

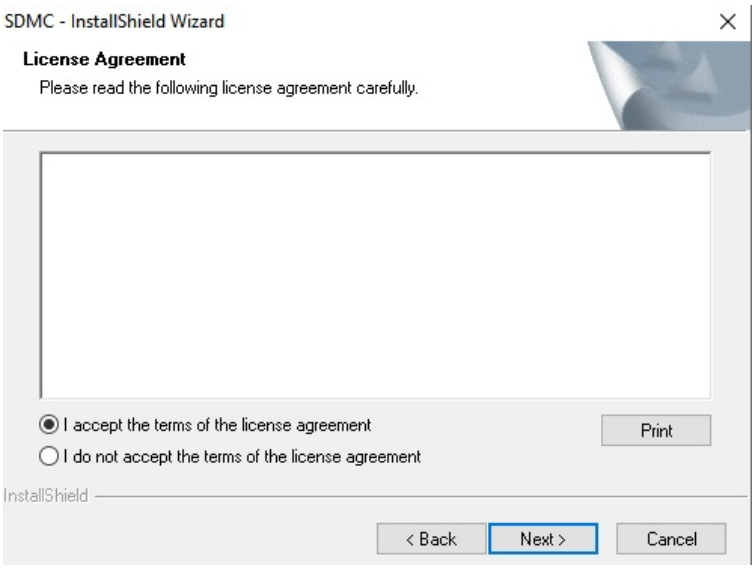
1. Decompress the SDMC zip file
2. Click the setup.exe file.
3. Click “**Yes**” in the pop-out window to continue the installation.



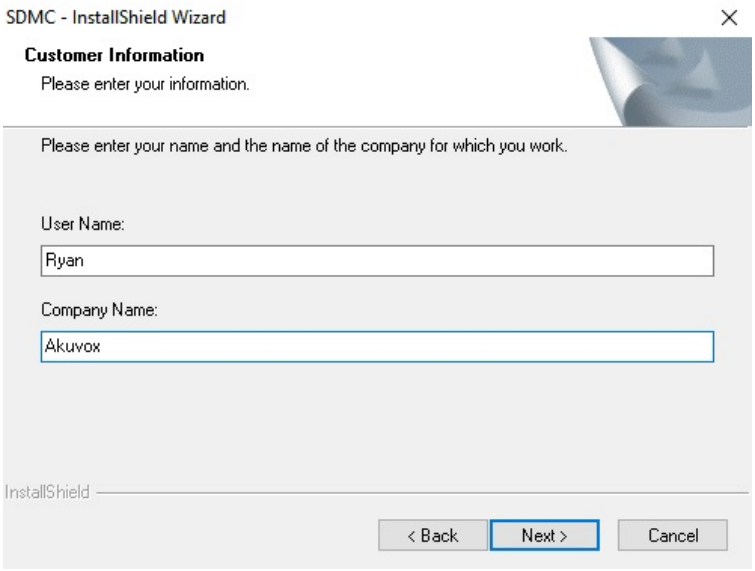
4.Click “**Next**” to go to the next step



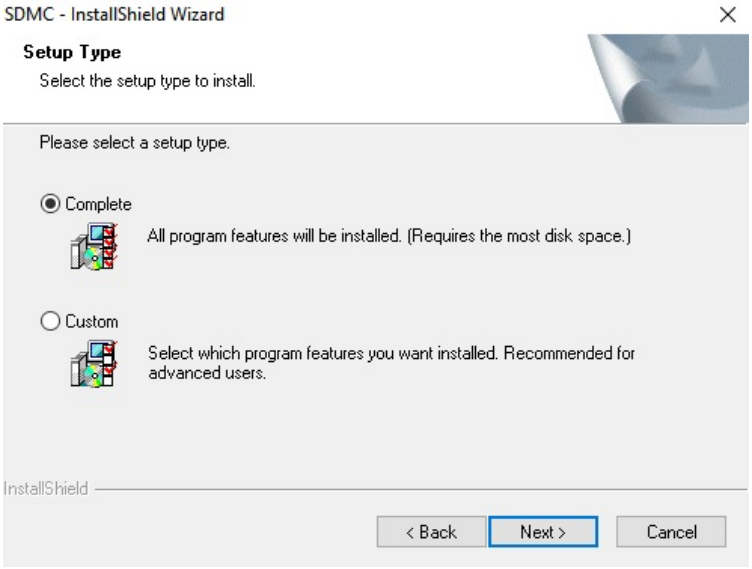
5. Click to accept the terms and Click **Next** to accept the agreement.



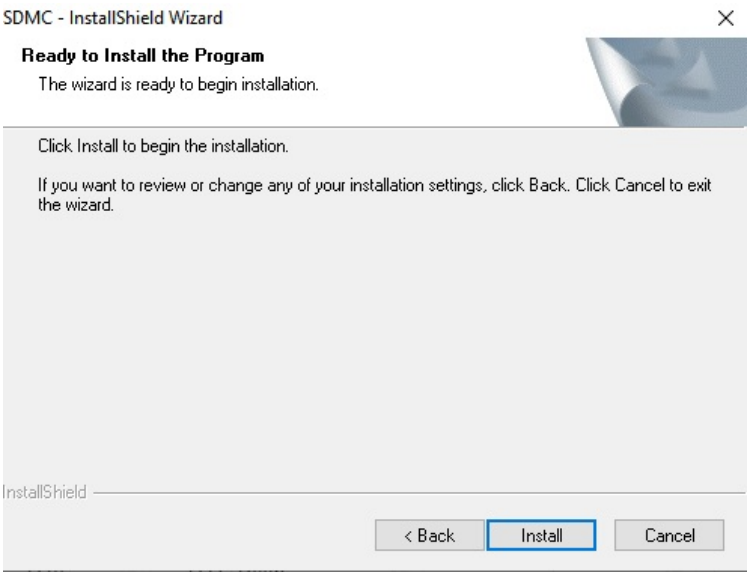
6.Enter the **User Name** and **Company Name** and click **“Next”.**



7.Select the installation path by default or the other path to your preference and click "**Next**".



8.Click "**Install**" to finish the installation.



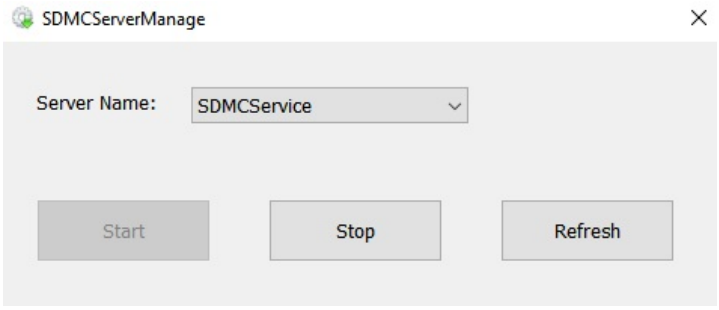
After the installation is completed, you will see the SDMC icon along with SDMC SeverManage icon on your desktop.

Note:

- The SDMC installation path should not contain any Chinese characters.

2.3. Set up SDMC Server Manage Software

SDMC ServerManage is a program that is installed along with the SDMC. The software is designed to manage types of services called “SDMC Service”, and “WatchdogService”.

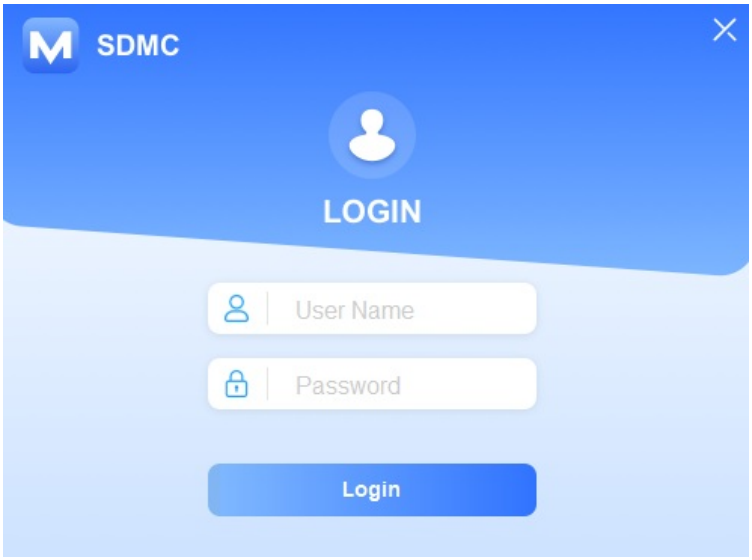


- **SDMC Service:** this service is used to facilitate the two-way communication between the SDMC and the devices for the data transmission, therefore the service must be turned on to ensure the smooth running of SDMC
- **WatchdogService**: Watchdog will be running automatically upon the completion of its installation by default. **WatchdogService** is responsible for monitoring the SDMC **Sevice** status. To be more specific, **Watchdog** will turn on **SDMCService** automatically whenever it finds **SDMCService** is not running, which means **SDMCervice** will be running nonstop or will be up and running again on condition that the Watchdog is on.

3.Log in SDMC

To log in SDMC for the first time, you are required to enter the username “**admin”**, and the password ”**admin**” by default. While you can click

on the upper right corner of the screen to close SDMC.

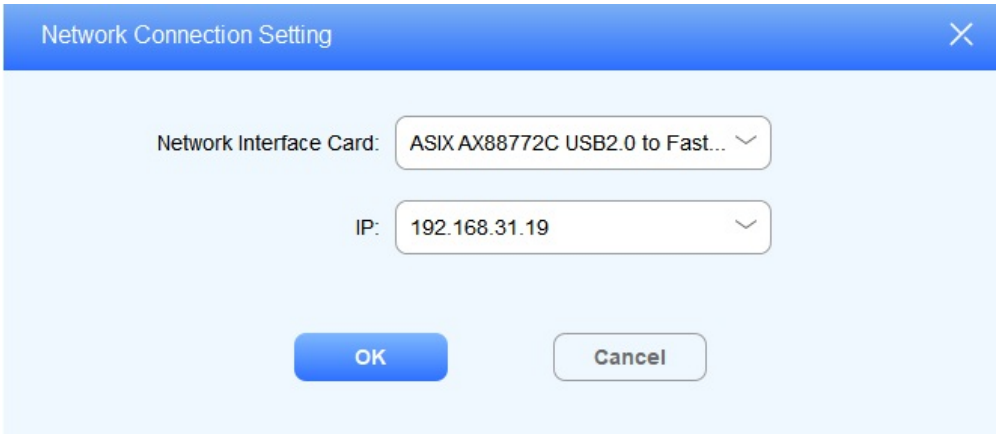


4.Getting Started

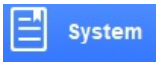
4.1. Configure SDMC Network Connection

You need to select specific NIC (Network Interface Card) used to connect SDMC and devices for the data transmission. And SDMC IP address will appear automatically after you select your NIC.

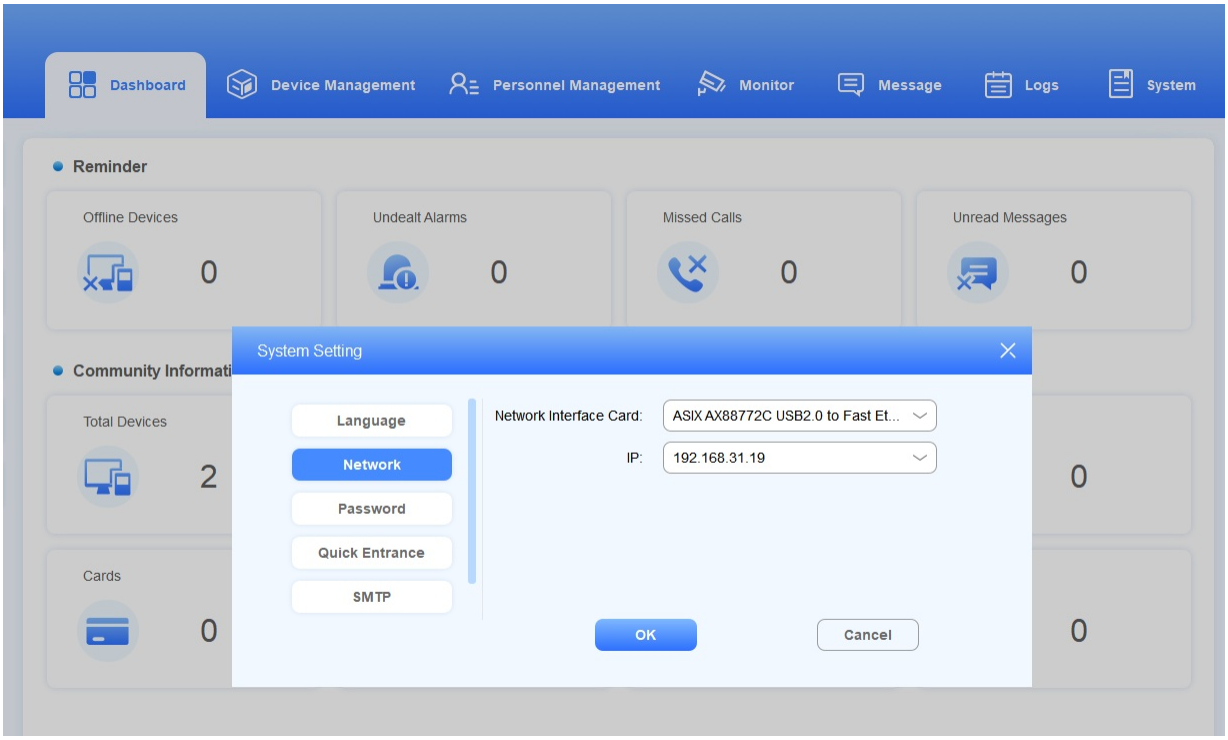
1. Click to select NIC (which is the network adaptor in your computer), and you will see the corresponding IP address what appears automatically when network adaptor is selected.



2.You can also click



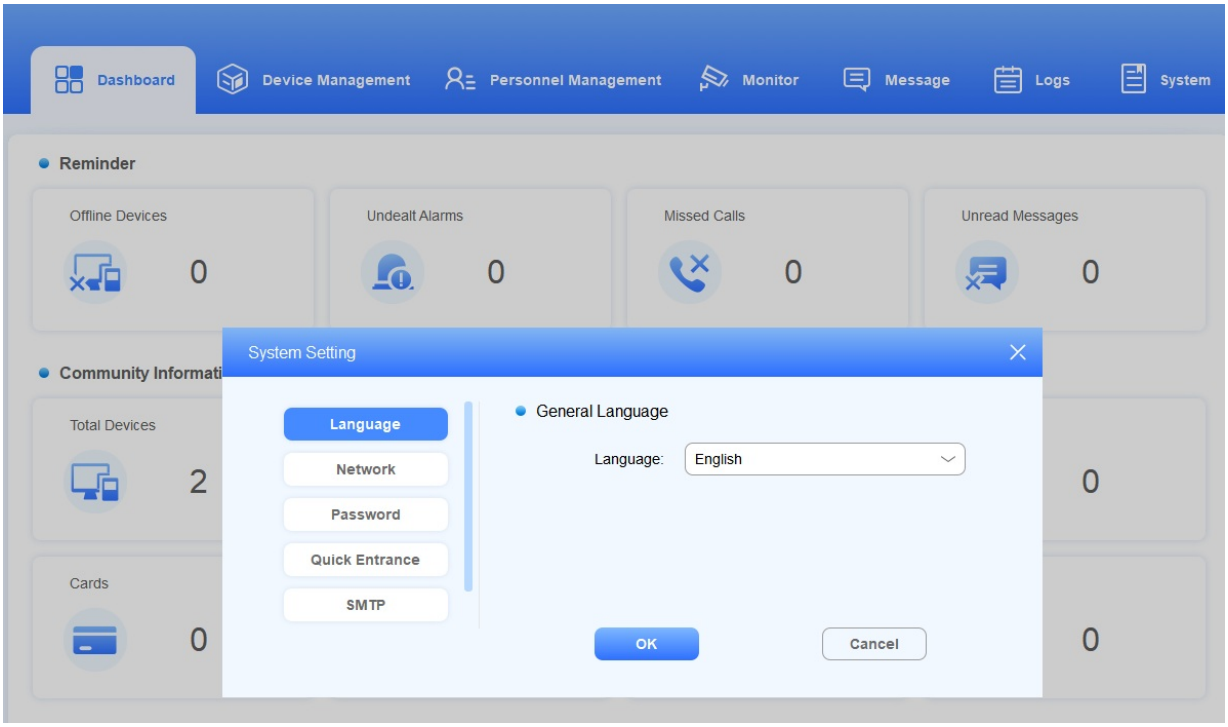
, select **System Setting > Network** to set and edit the network connection after login.



4.2. Language

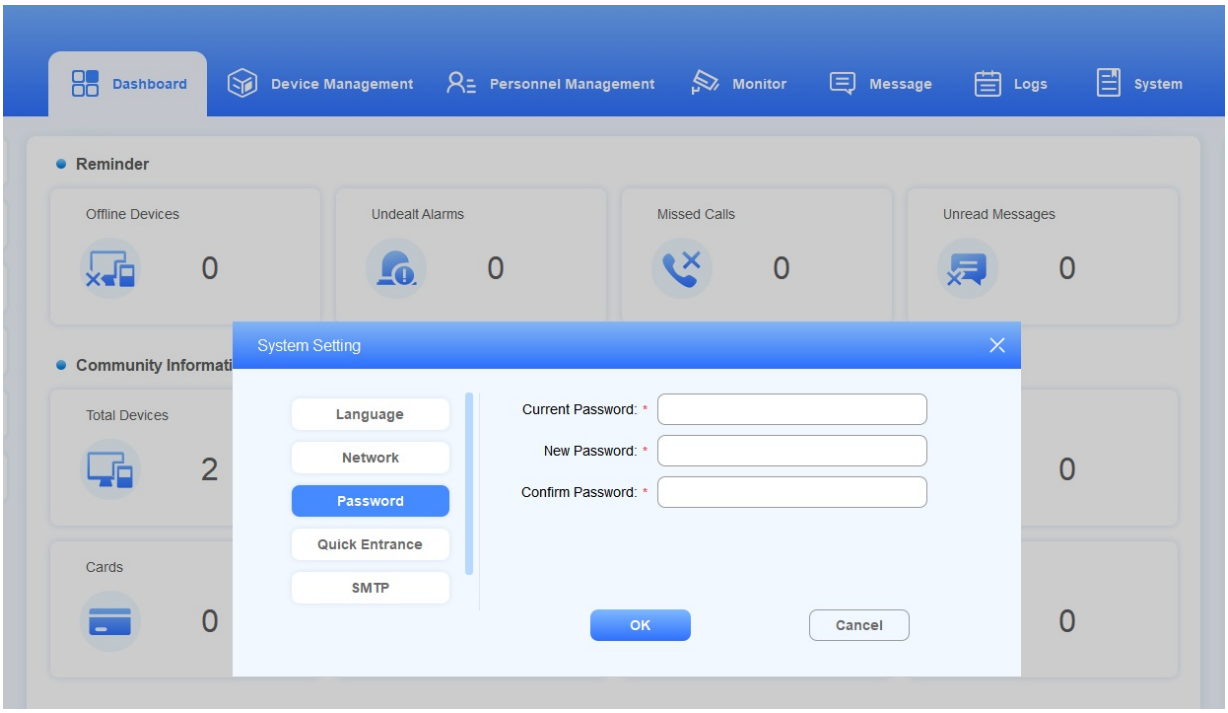
SDMC currently supports English and Chinese languages (both simplified and traditional Chinese character). You can select either of them according to your need.

1. Click on **System** module, then select **System Setting > Language**.
2. Click **OK** for the Confirmation.



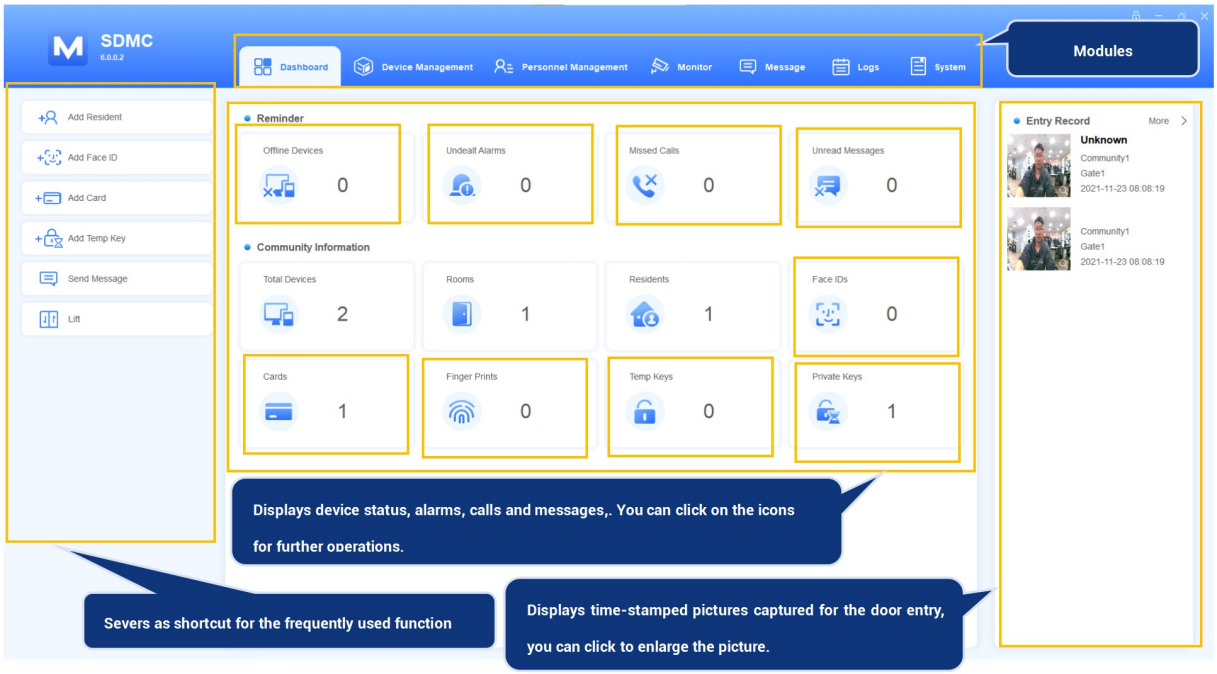
4.3. Password

After you log in to the SDMC, you can change the SDMC login password if needed.



5.Dashboard

SDMC dashboard is mainly consisted of Seven modules, namely **Dashboard**, **Device Management**, **Personnel Management** , **Monitor**, **Message**, **Logs**, and **System** along with two functional columns on both sides.



Modules

- **Modules**

NO.	Modules	Descriptions
1	**Dashboard**	Gives you a quick view of real-time statistical information on device, calls, messages , residents, and different types of entry records etc.
2	**Device Management**	Allows you to create nodes to which you add, edit and delete devices. You can also modify certain device setting before synchronizing the changes to the devices. More over, you can make call to a specific device and unlock the door if needed.
3	**Personnel Management**	Allows you to manage access control for the residents and property management, to manage various types of access authentication methods for staff, residents and visitors etc.
4	**Monitor**	Allows you to manage monitoring devices in terms adding, edit and deleting monitoring devices and to perform monitoring video preview.
5	**Message**	Allows you to manage messages and notification ads etc.
6	**Logs**	Allows you to manage various types of logs such as access logs, alarm logs, call logs, system logs.
7	**System**	Allows you to manage SDMC SIP setting, Atop data backup, lift control, network,language,password,dashboard operation icons on the left column, SMTP, and device reset and reboot.

6.Device Management

In the device management module, you can manage device deployment on the node basis, and synchronize the data to the corresponding devices at different nodes you selected. While you can make call to the specific device and to unlock the door if needed. In addition, you can search and check data for the specific device(s).

6.1. Create Deployment Nodes

You are required to create nodes first before you can deploy the devices to the nodes you set up. You can either manage the node one by one or using a template. A community can extend to a total of six nodes for the device deployment.

- **About Nodes**

NO.	Node	Descriptions
1	**Community**	Community is the root nodes which is extendable to other five subordinating nodes: “**Public/ Building > Unit >Floor > Room**. Public and Building are parallel nodes.

2	**Public**	Public is also the second level of nodes. You c an create **1-99** public nodes maximum.
B u il d i n g	Building is second level of node, which can b e extensible to other three subordinating node s “**Unit >Floor > Room**”. You can create **1-999** building nodes maximum.	
3	**Unit**	Unit is the third level of node, which can be ex tensible to other two subordinating nodes “**Flo or > Room**”. You can create **1-99** unit nodes maximum.
4	**Floor**	Floor is the fourth level of node, which can be extensible to **Room** node. You can create **1-9 9** unit nodes maximum.
5	**Room**	Room is the lowest level of node. You can cre ate **1-99** room nodes maximum.

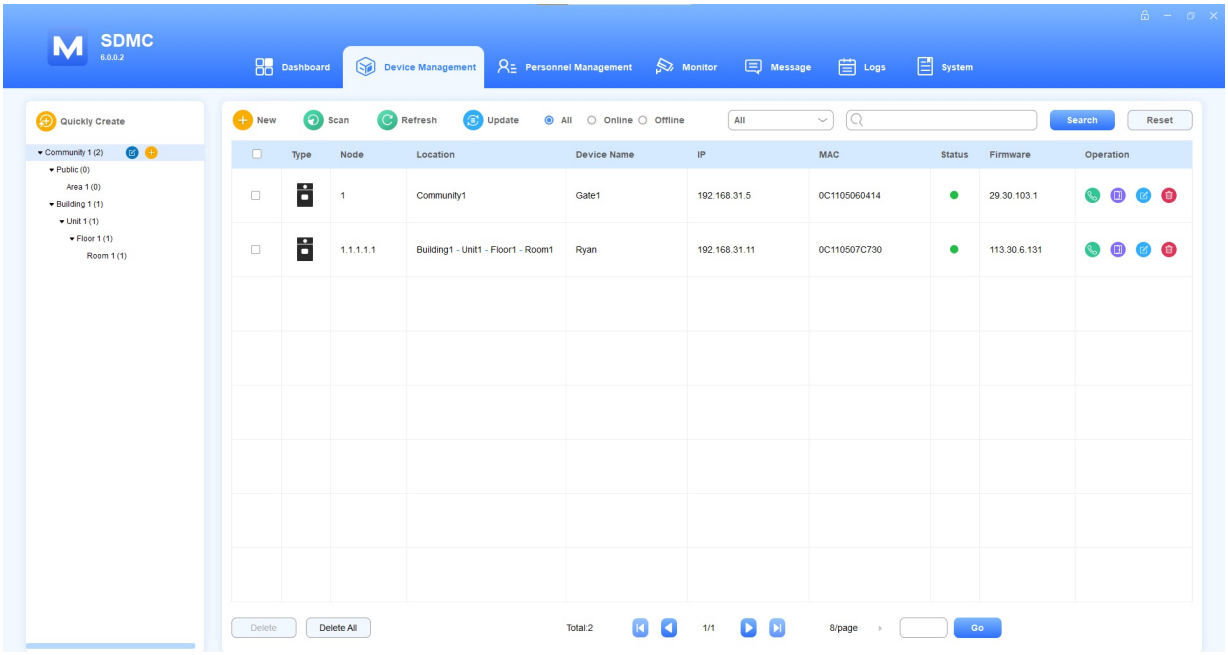
6.1.1. Add Nodes Separately

You can create nodes in the **Device Management** Module. You can create the nodes from community node all the way down to room node.

1. Move the arrow to the **Community** (root node), and click 

   beside the node to create building nodes
2. After the building nodes is created, you can create other nodes subordinated to the building nodes in the same way.
3. Move the arrow to Public node and click 

   beside the node to create public area node.



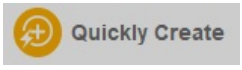
Note:

You can click

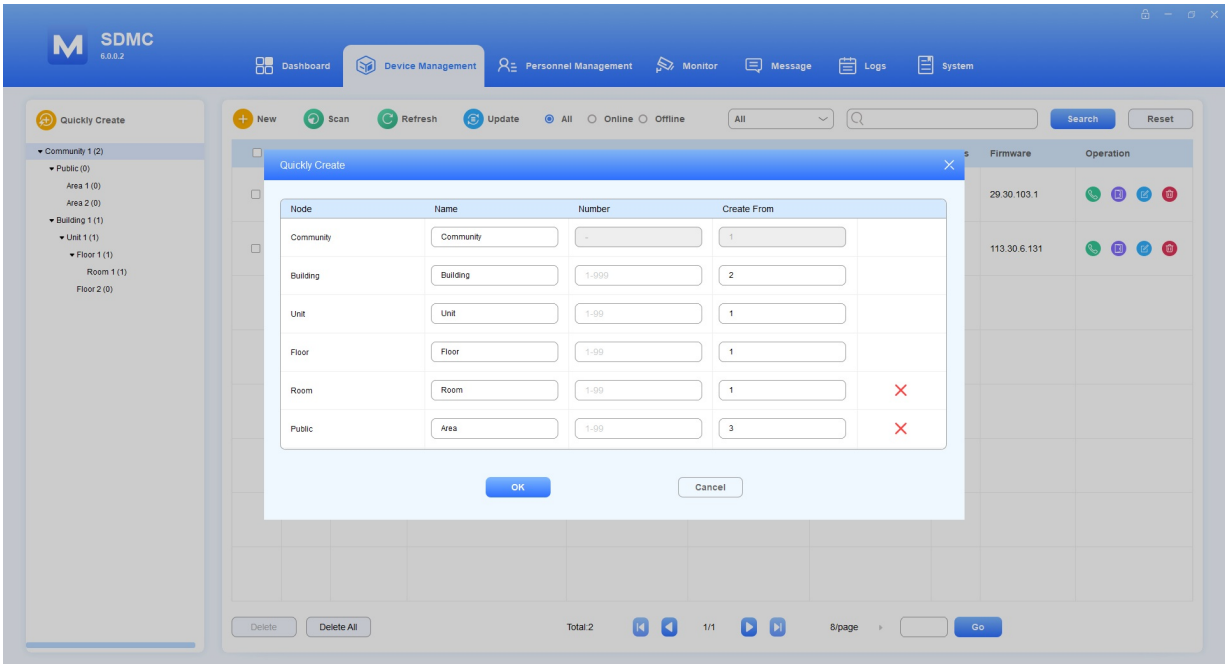
to change the node name if needed.

6.1.2.Add Node Using Template

1. Click

   to go to the node template.
2. Set up the number nodes at each node level according to your need



Note:

- You can change the node name if need.
- Room and public nodes are optional

6.2.Edit/Delete Nodes

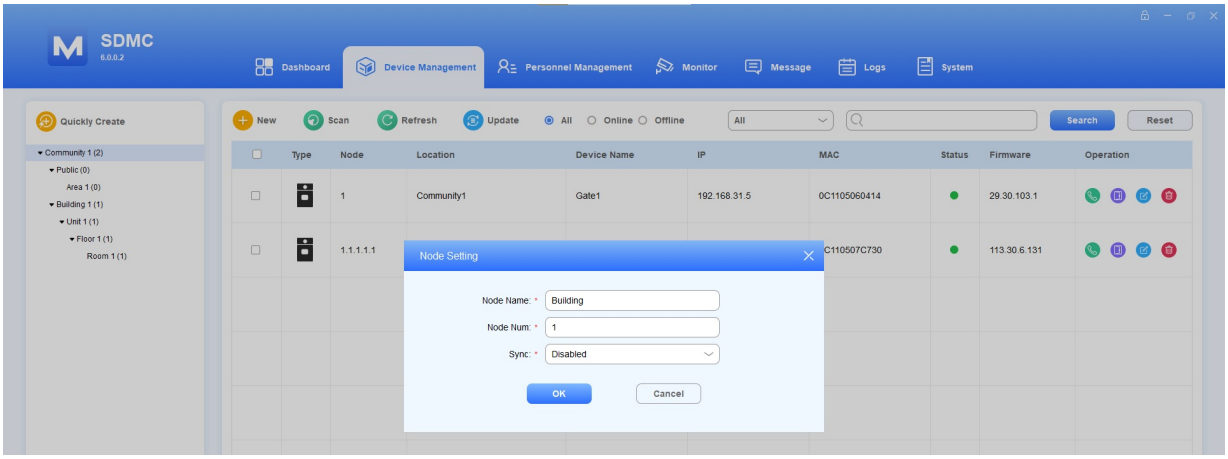
You can edit nodes in terms of their names and node numbers. And you can delete the node if needed.

1. Click

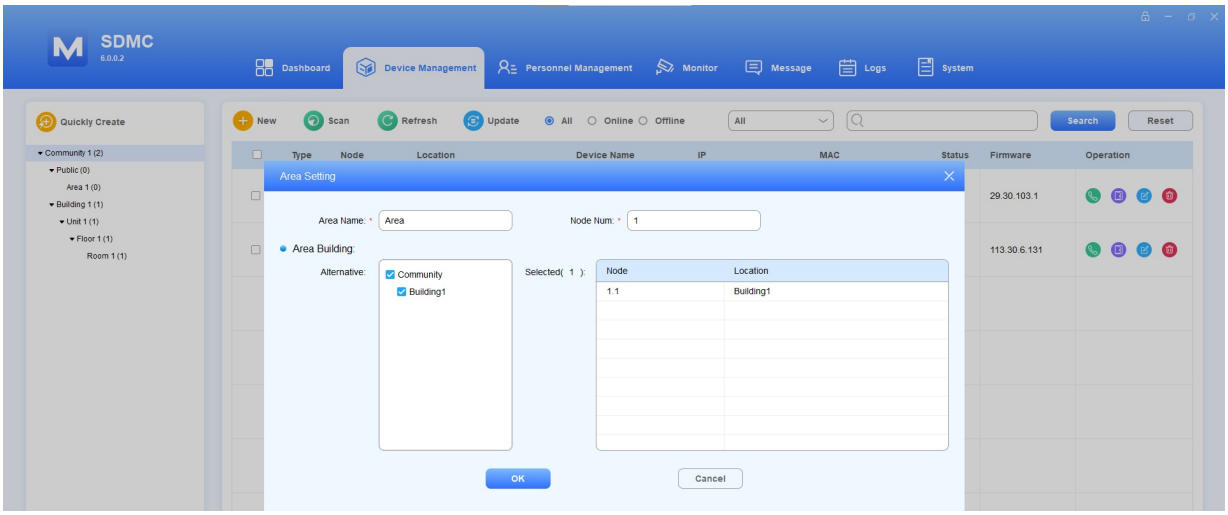
   of the node you want to edit.
2. Change the node name and number if needed.
3. Select “**Enable**” in the Sync field if you want to synchronize the name changes to all the parallel node at the same node level, adopting the same name. For example, if you change the building 1 to be building A then all the building nodes will change their name to “ **Building A**” after synchronization.
4. Click

   of the node you want to delete.

- **Building Node**



- **Public Node**



Note:

- You can change the node name if need.
- Room and public nodes are optional

6.3. Add Device

After the nodes are created, you can start adding the device(s) to the specific level of nodes in the **Device Management** module.You are required to fill in all of the device network information etc. While you can also configure and synchronize the device settings to the device(s) if needed.

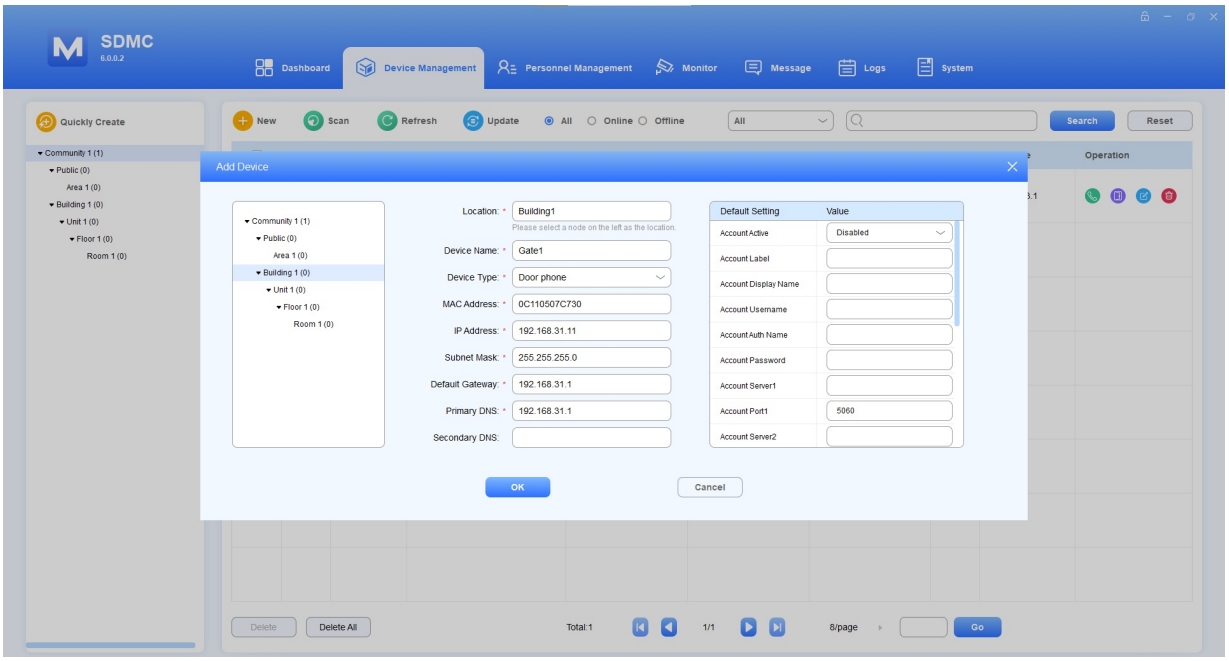
Device can be added manually or added via scanning.

6.3.1. Add Device Manually

1. In the **Device Management** Module, click

.

2. Select the specific node to which you want add the device.
3. Fill in the device name, type and network parameters
4. Configure and synchronize the device setting to the device if needed.



- **Parameter Description:**

NO.	Parameter	Description
1	Location	Click and select the node, then the location field will be automatically filled in.
3	Device Name	Fill the the device name, for example the device location name for the identification purpose. The maximum field length is 63 digits. If you leave the device name blank, then the system will prompt “ Please input name”.
4	Device Type	Select device type: Indoor monitor, Door Phone, Video Phone, and Access control. The default device type is “ Door Phone”.
5	MAC address	Fill in the device MAC Address.
6	IP Address	Fill in the device IP address.
7	Subnet Mask	Fill in the device Subnet Mask.

8	Default Gateway	Fill in the device default gateway.
9	Primary DNS	Fill in the primary DNS.
10	Secondary DNS	Fill in the secondary DNS.

Note:

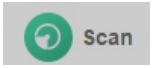
- Device network setting can be obtained on the device.
- **SDMC Device Configuration**

NO.	Settings	Description
1	Account Active	Enable or disable the device SIP account.
2	Account Label	Fill in the device SIP account display label.
3	Account Display Name	Fill in the device SIP account display label.
4	Account Username	Fill in the device SIP account User name, which can be the same with account SIP account authentication name.
5	Account Auth Name	Fill in the device SIP account authentication name.
6	Account Password	Fill in the device SIP account authentication passwords
7	Account Server1/2	Fill SIP server IP address.
8	Account Port1/2	Fill the SIP server port for the data transmission. The default SIP server port is 5060.

9	RTSP Enable	Enable the RTSP if you want to obtain the video footage from the device.
10	Prevent SIP Hacking	Enable it if you want to deny the call from other devices which does not share the same SIP server with called-party device.
11	DTMF Option	Select the number of DTMF digit for the door access control (Ranging from 1- 4 digits) For example, you can select 1 digit DTMF code or 2-digit DTMF code etc., according to your need.
12	DTMF Code 1/2/3	Set the three sets of DTMF codes for relay A/B/C. and the number of the codes depends on your DTMF option.
13	Relay Enable	Enable the open relay via HTTP function.
14	Relay UserName	Create authentication name for the open relay via HTTP. Relay username must be configured before you can unlock the door via HTTP on SDMC.
15	Relay Password	Create password for the open via HTTP authentication. Relay password must be set before you can unlock relay via HTTP on SDMC.

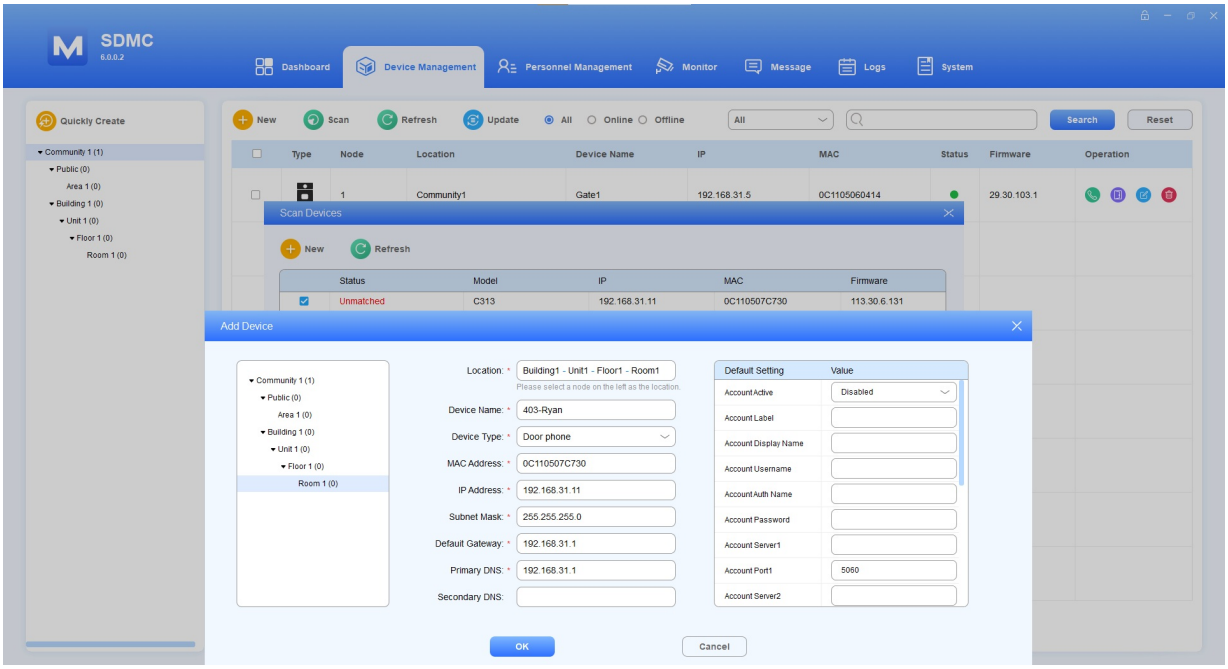
6.3.2.Add Device via Scanning

SDMC allows you to scan the devices in the same network before adding them to the specific node. Device network information will be automatically filled in.

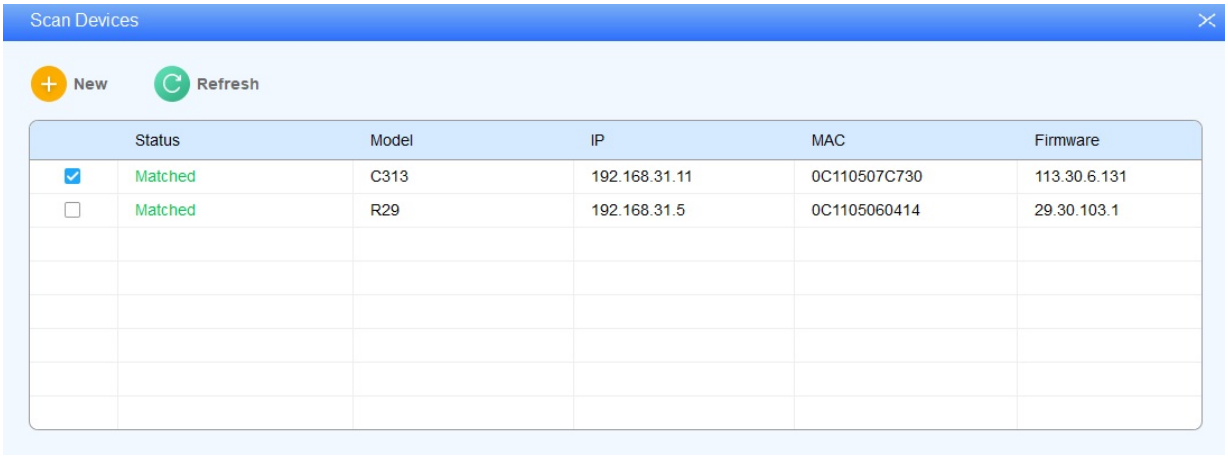
1. In the **Device Management** module, click
   

2. Tick the checkbox
   
   of the specific device you want to add, then click
   

   .
3. Click to select the specific node to which you want to add the device, and complete the setting in the same way as you do it manually.



After the device is added successfully, it will show "**Matched**".

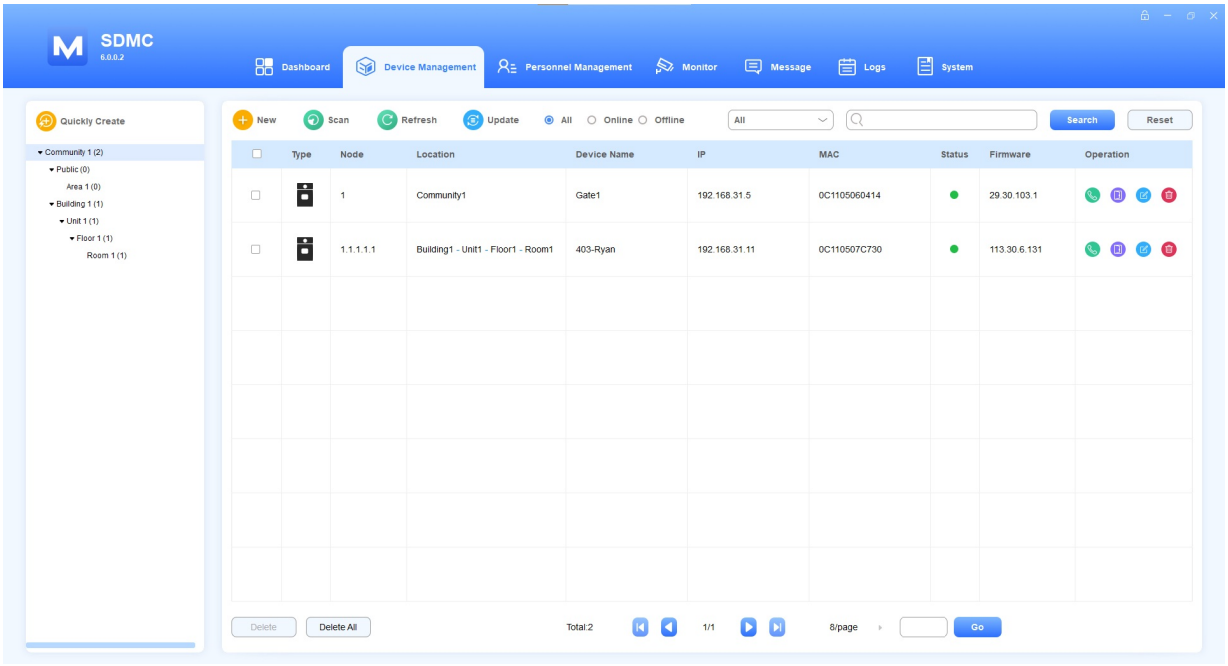


6.3.3.Check/Edit/Delete Device

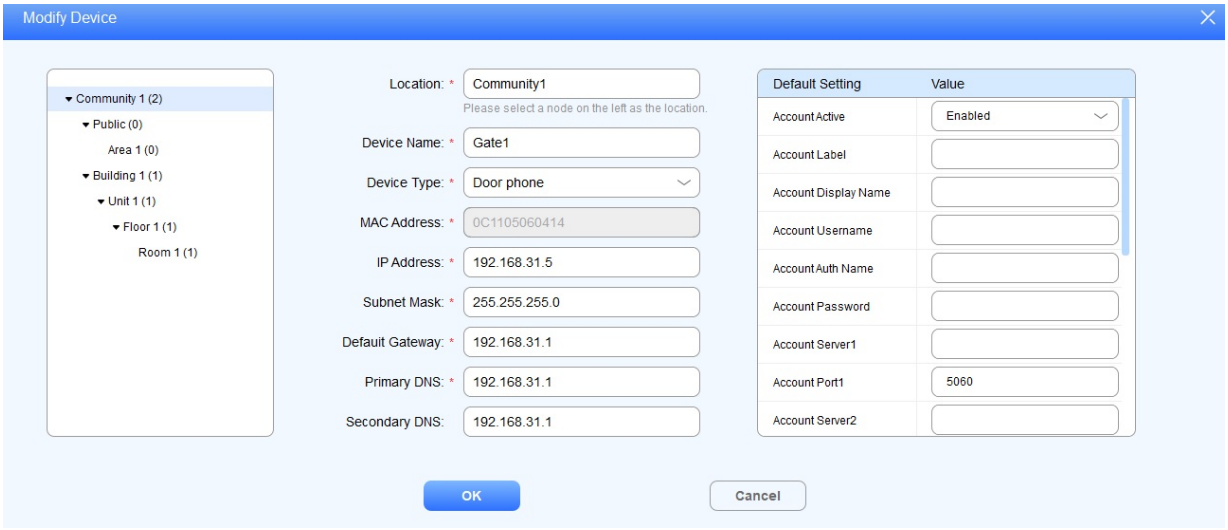
1. search and check the device by device online status, device type, keyword.
2. Click

   of the specific device you want to delete
3. Click

   of the specific device you want to edit.



4.Edit the device in terms of moving the device to the different node and modifying device network, device type, device name, device node name and configurations etc.



- **Field Name Description**

NO.	Field Name	Description
1	Type	Indicates the device type.
2	Node	Indicates the level of node at which the device is deployed.
3	Location	Indicates the device locations corresponding to the nodes.
4	Device Name	Indicates the device name.
5	IP	Displays device IP address.
6	MAC	Displays device MAC address.
7	Status	Displays device online status.
8	Firmware	Display the current device firmware version

9	Operations	Allows you to the perform four operations :

6.3.4. Make Call to Device

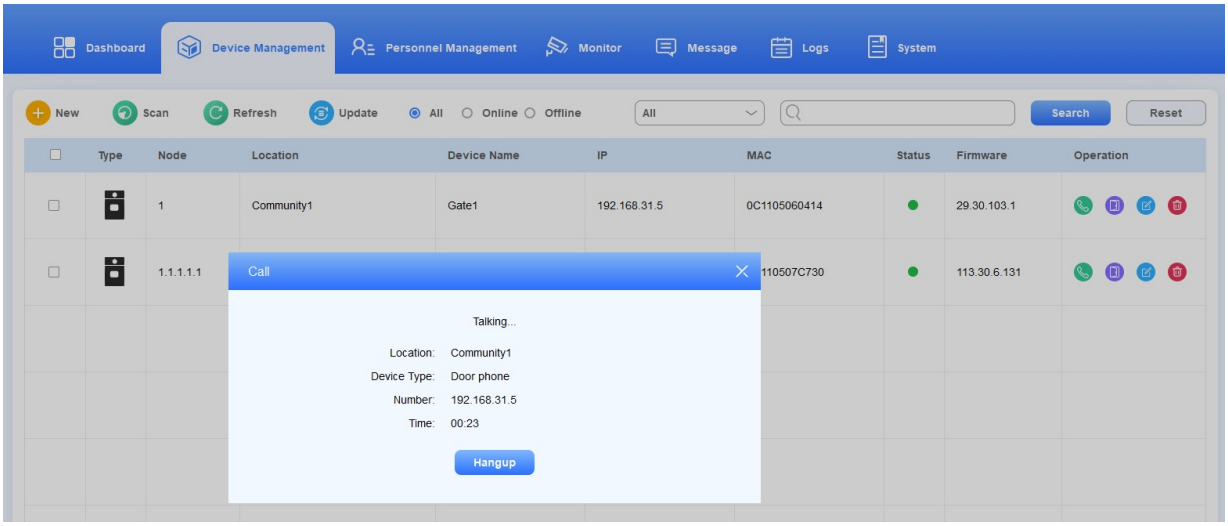
As an administrator, you can make call to the specific device if needed.

1. Click

   of the specific device.
2. Click

   Hangup

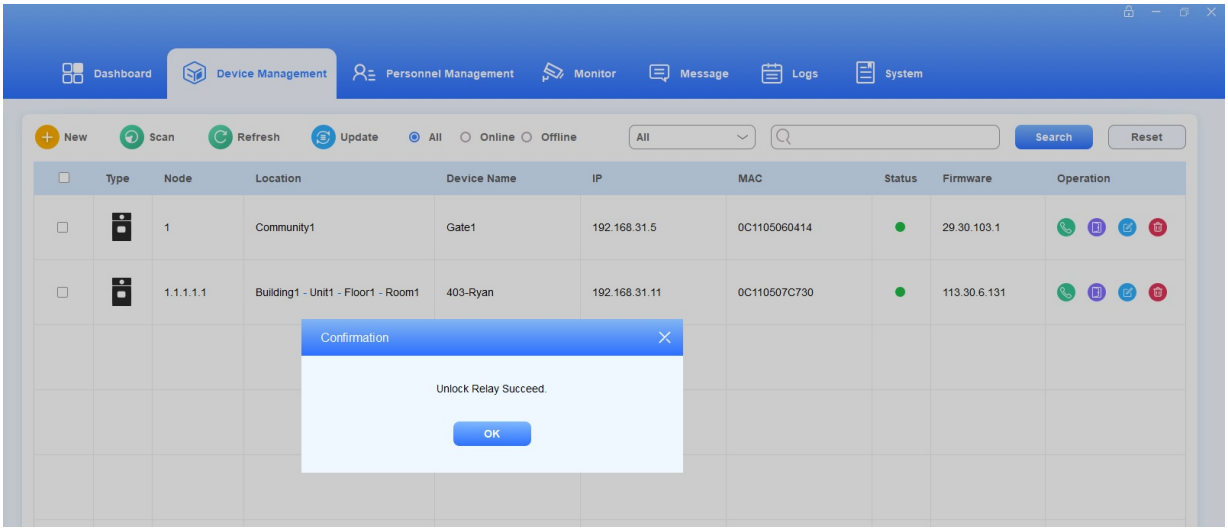
   to hang up the call.



6.3.5. Unlock Device Relay via HTTP

1. Click

   of the specific device.



7.Personnel Management

Personnel Management module includes three sub-modules, namely Resident manager, Property Worker Manager, and verification mode manager. With these sub-modules, you will be able to achieve a complete management of residents, property staff, various type of authentication, and access control.

7.1. Manage Resident

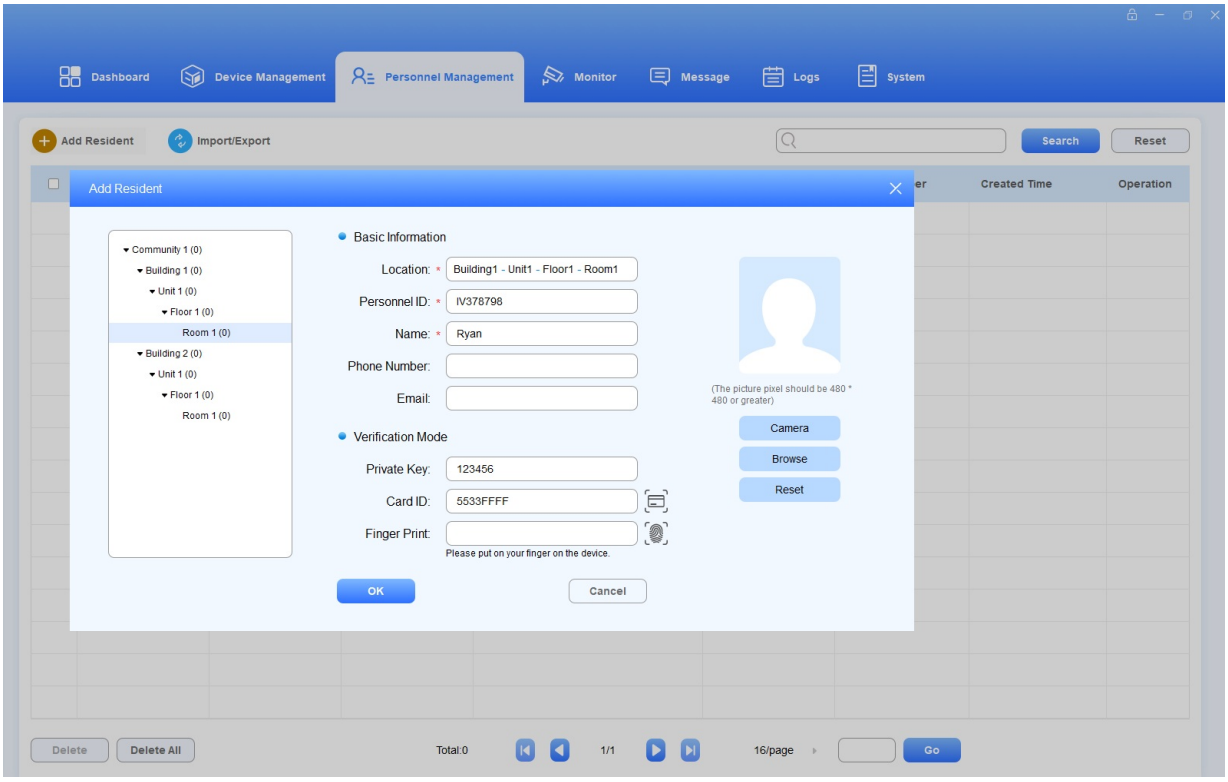
You can add residents to their corresponding locations by rooms and building etc while managing their personal information and grant them various type of access method for the access control.

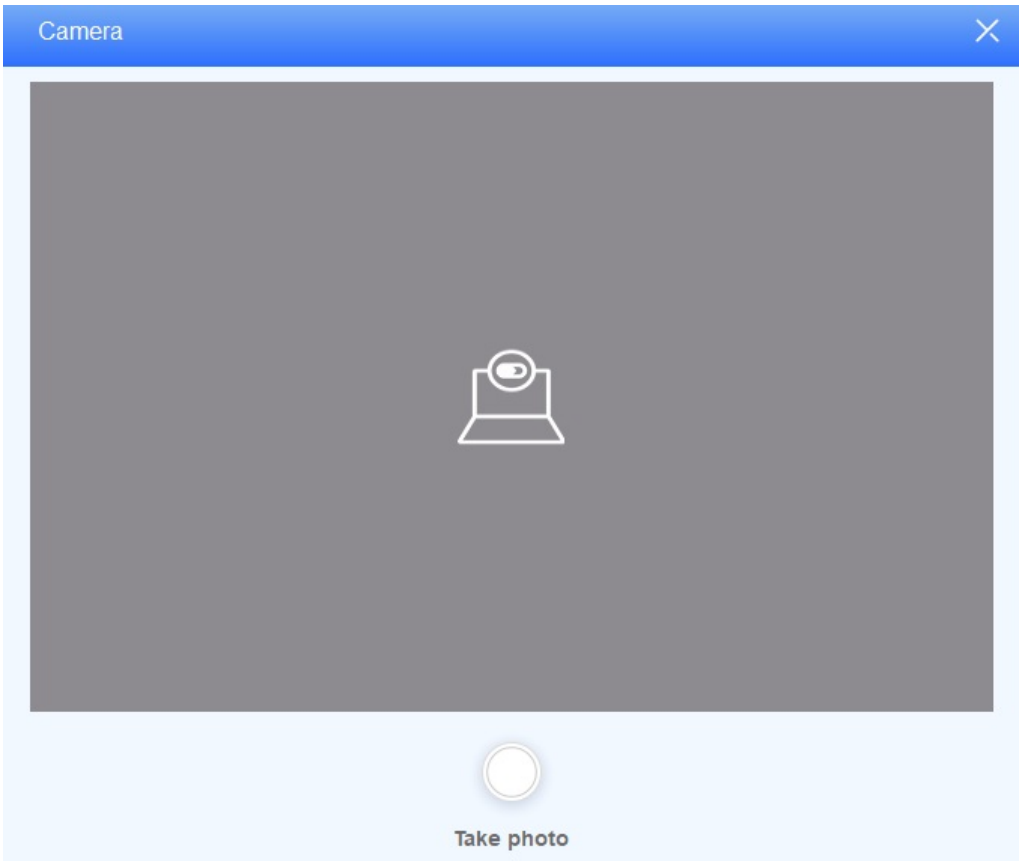
7.1.1. Add Resident

You can add resident to the rooms and building on the node basis.

1. Click **Personnel Management** module, and select **ResidentManager,** then click 

.
2. Select specific room node at which you want to add the resident.
3. Enter the resident's personal information.
4. Set access authentication methods for the resident:
5. Create the private PIN code.
6. Click 
to obtain the ID card number from the card reader connected to the SDMC, or enter the ID card number directly.
7. Click 
to obtain the figure print from the finger print reader connected to the SDMC.
8. Upload Resident Face ID for access authentication.
9. Click **Browse** to upload the resident's picture, and reset the picture for re-upload if needed.
10. Click **Camera** to take a picture of the resident before uploading.





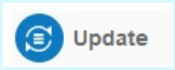
- **Field Name Description:**

NO.	Field Name	Description
1	Location	Location can only be the room node (the lowest node)
2	Personnel ID	Personnel ID can be automatically generated, or you can change the personnel ID when adding the resident.
3	Name	You can only enter 63 characters maximum in length.
6	Phone	You can only enter 63 characters maximum in length.
5	Email	You can only enter 63 characters maximum in length.

6	Private Key	Private PIN code should be 2-8 digits
7	Card ID	You can only enter number or alphabet with 127 digits in length. Each resident can be assigned with five card numbers maximum. And card numbers should be separated by ";"
8	Finger Print	Scan your finger on the finger print reader.
9	Face ID	You can upload the face ID directly, or you can take a picture of the resident with your PC camera (the picture should be 480*480 or greater). Face in the picture should be clear and in front-view, accounting for 1/4 of the total space of the picture.

Note:

After the resident information and authentication methods are set up, you are required to click

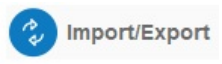


in the Device Management Module to synchronize the data to the device.

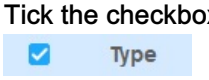
7.1.2.Import/Export Resident Data

You can import the .zip file to SDMC to quickly set up resident's information and access authentication methods and export the zip file as needed for backup for later use etc.

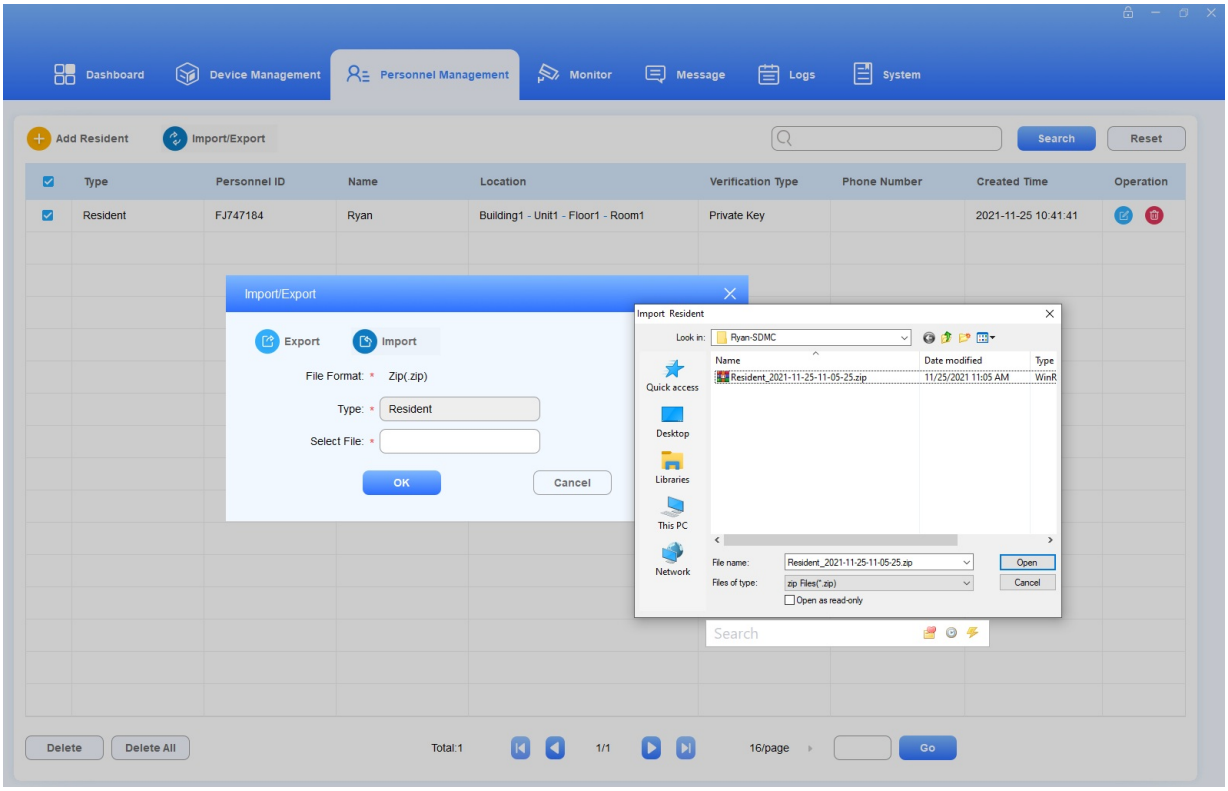
1. Click

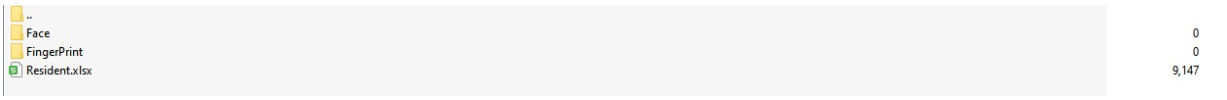
   .
2. Click **Import**, and select the .zip file in your local PC, then upload the file to your SDMC.
3. Tick the checkbox of the specific resident(s) or tick

   of all the resident, then click Export and select where you want to store the .zip file in your PC, then click **Save**.



- **.Zip file sample**



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Index	Location	PersonnelT	PersonnelI	Name	PhoneNum	Email	PrivateKey	CardID	FingerPrint	FaceID			
2	1	Communit	Resident	FJ747184	Ryan			123456						
3														
4														
5														

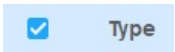
Note:

You are allowed to upload .xlsx excel file to the SDMC directly if you do not need to import face and finger print data.

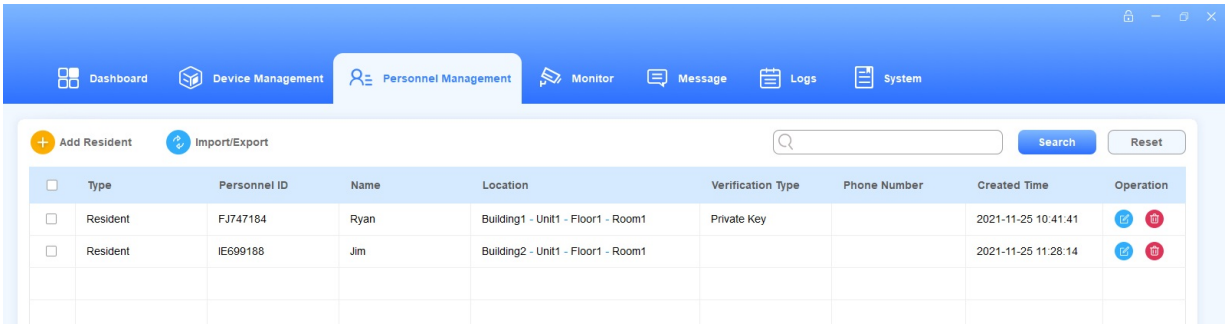
7.1.3.Check/Edit/Delete Resident

You can search, check, edit and delete the residents that have been added.

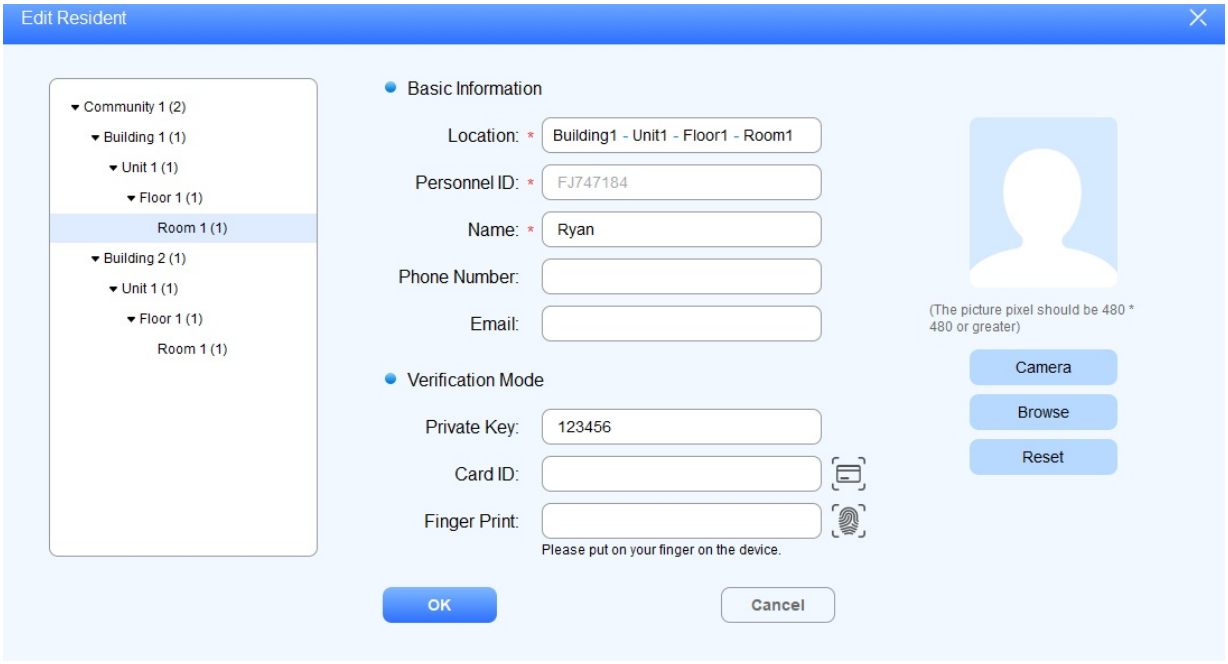
1. Search the resident by **Personnel ID**,**Name**, **Location**, **Phone Number** in the Fuzzy search field
2. Tick the checkbox of the specific resident(s) or tick the



if you want to delete all the residents



3.Tick the checkbox of specific resident you want to edit.

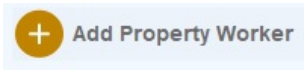


7.2.Manage Property Staff

7.2.1.Add Property Staff

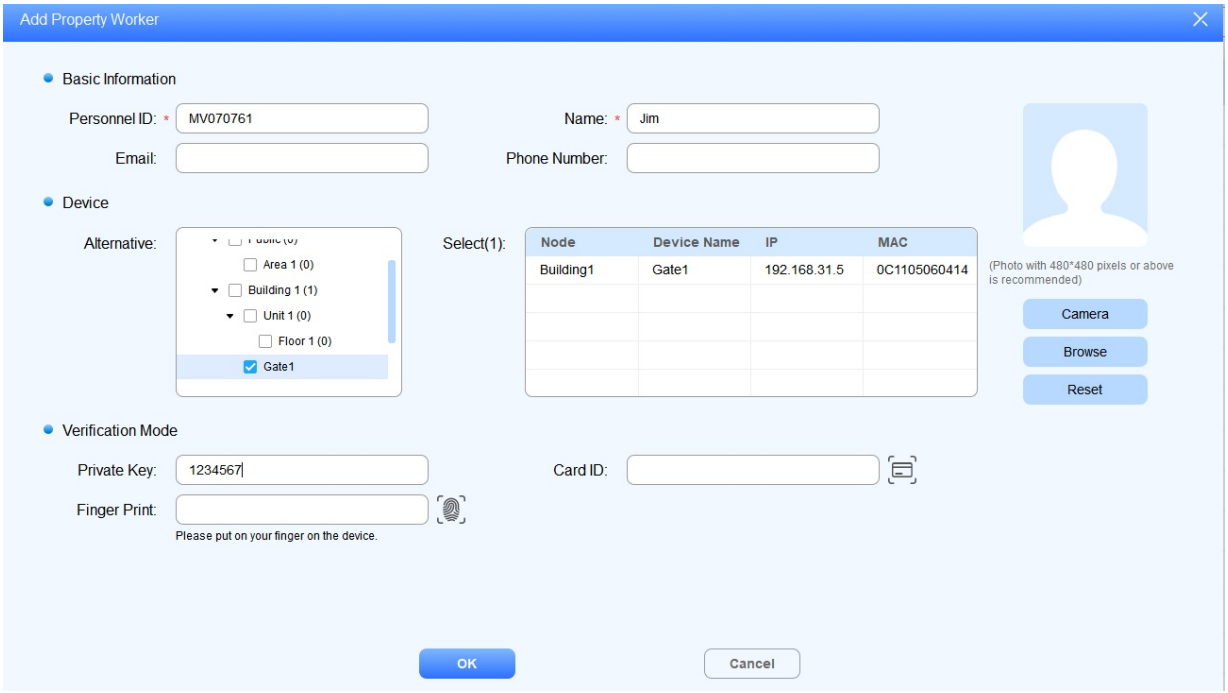
You can add property staff(s) and grant them the permission to unlock the doors or gates in the specific location for the property management.

1. Click **Personal Management** Module, and **select Property Worker Manager.**
2. Click



.

3. Enter the staff's personal information and change the automatically generated personnel ID if needed.
4. Grant the staff the permission to access the specific door by selecting the specific access control device at the specific location.
5. Set the authentication methods for the staff in the same way as you do for the residents.



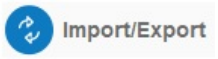
Note:

You can refer to chapter 7.2.2 for how to Set the authentication methods for the property staff

7.2.2.Import/Export Property Staff

You can import the .zip file to SDMC to quickly set up property staff information and access authentication methods, and export the zip file as needed for backup for later use etc.

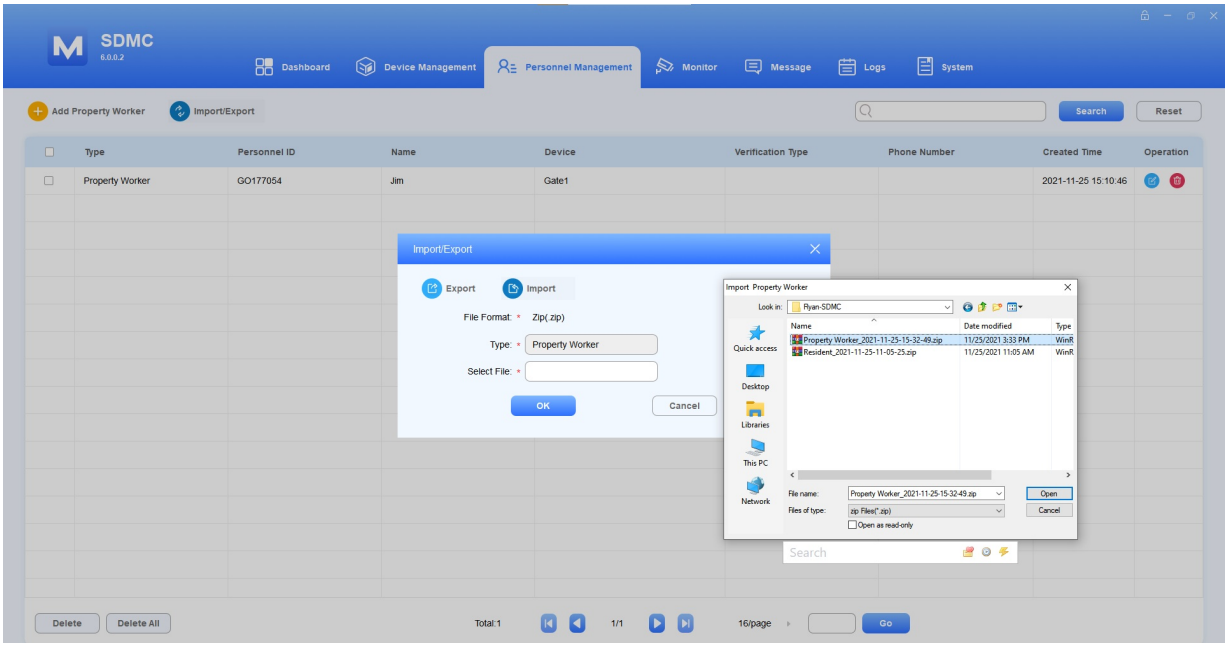
1. Click

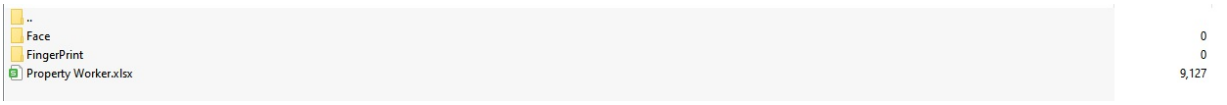
   .
2. Click **Import**, and select the .zip file in your local PC, then upload the file to your SDMC.
3. Tick the checkbox of the specific property staff(s) or tick

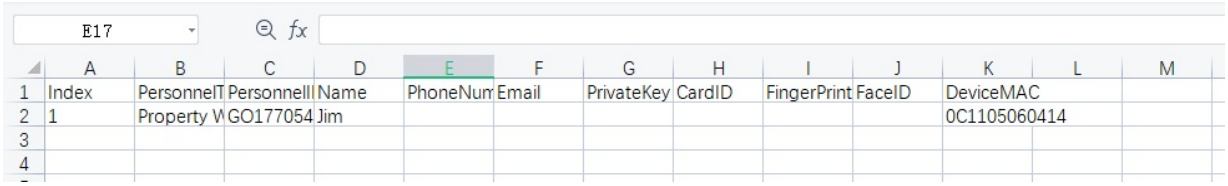
   

   of all the staffs, then click **Export** and select where you want to store the .zip file in your PC, then click **Save**.



- **.Zip file sample**





	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Index	PersonnelT	PersonnelI	Name	PhoneNum	Email	PrivateKey	CardID	FingerPrint	FaceID	DeviceMAC		
2	1	Property W	GO177054	Jim							0C1105060414		
3													
4													

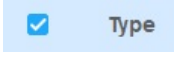
Note:

You are allowed to upload .xlsx excel file to the SDMC directly if you do not need to import face and finger print data.

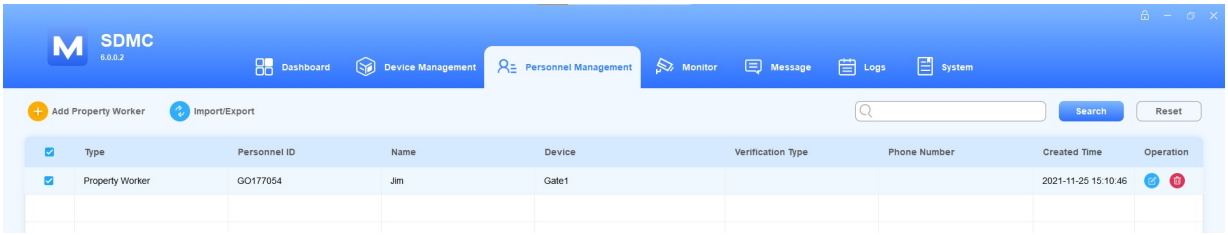
7.2.3.Check/Edit/Delete Property Staff

You can search, check, edit and delete the property staff that have been added if needed.

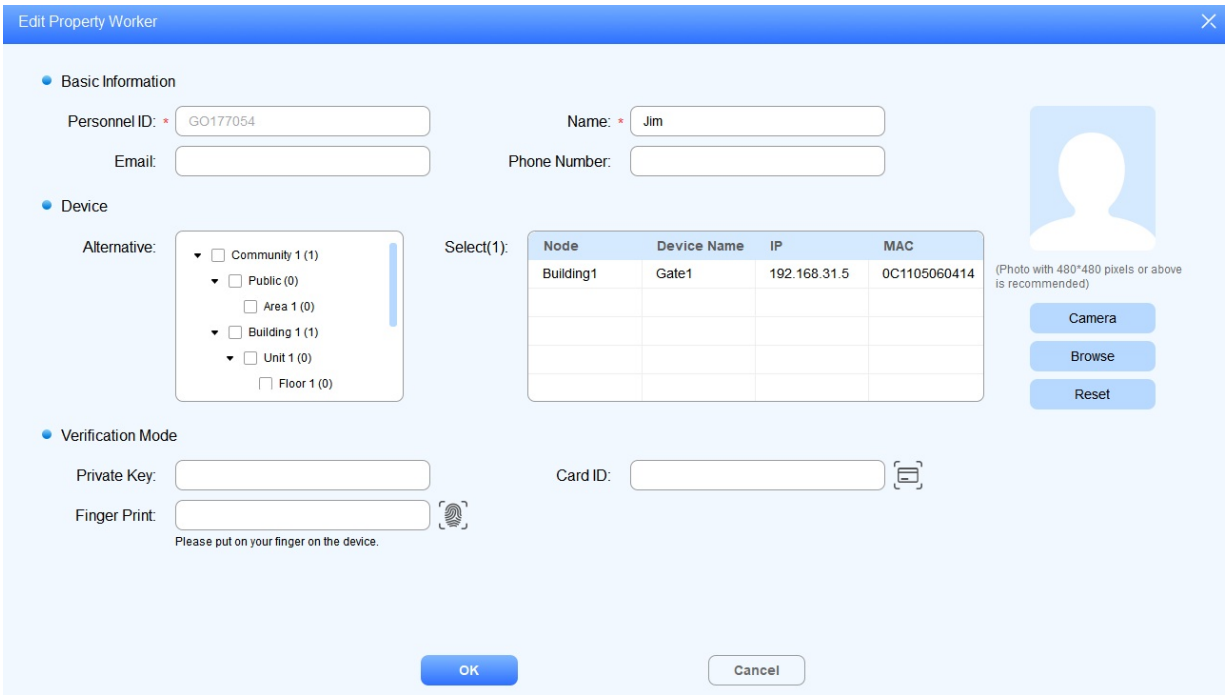
1. Search the property staff by **Personnel ID**,**Name**, **Location**, **Phone Number** in the Fuzzy search field if needed.
2. Tick the checkbox of the specific property staff(s) or tick

   the if you want to delete all the property staffs.



3.Tick the checkbox of the specific property staff you want to edit.



Note:

Keyword used for searching property staff are case-sensitive

7.3.Access Authentication Management

You can create various types of authentication methods to be used by both residents and property staffs. And you can designate the specific location(s) where you want them to gain access to.

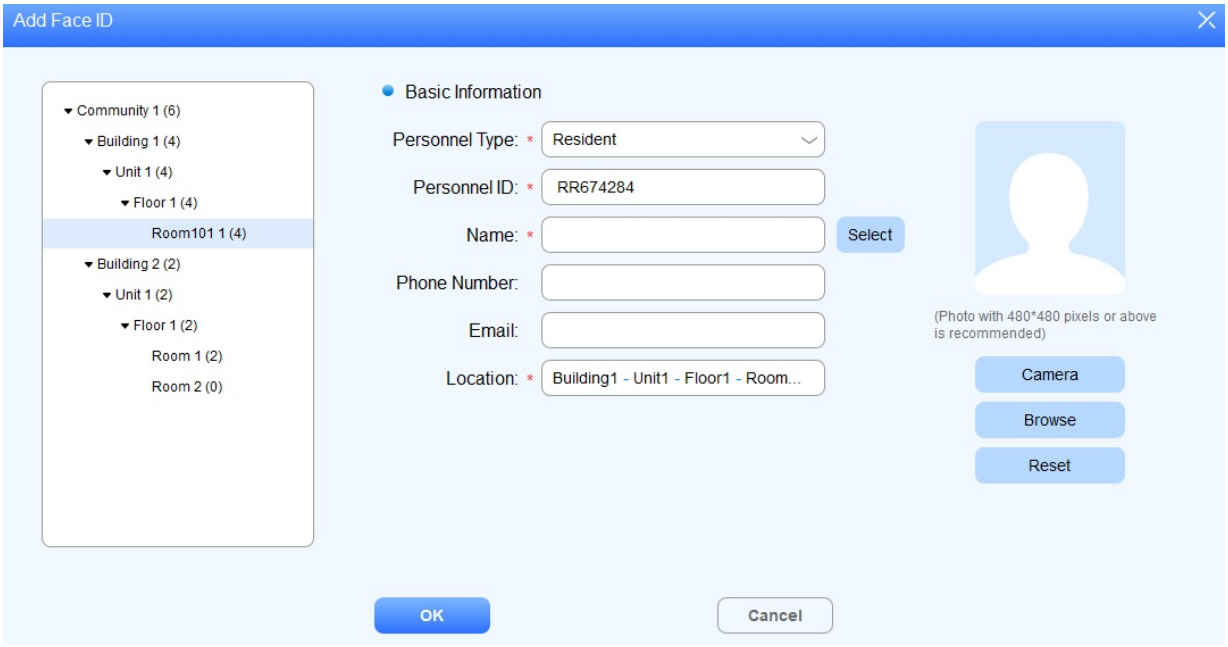
7.4.Face ID

7.4.1.Create Face ID

1. Navigate to **Personal Management > Verification Mode Manager > Face ID**
2. Click

   New

   .
3. Select Personnel Type.



- Select **“Resident”** type

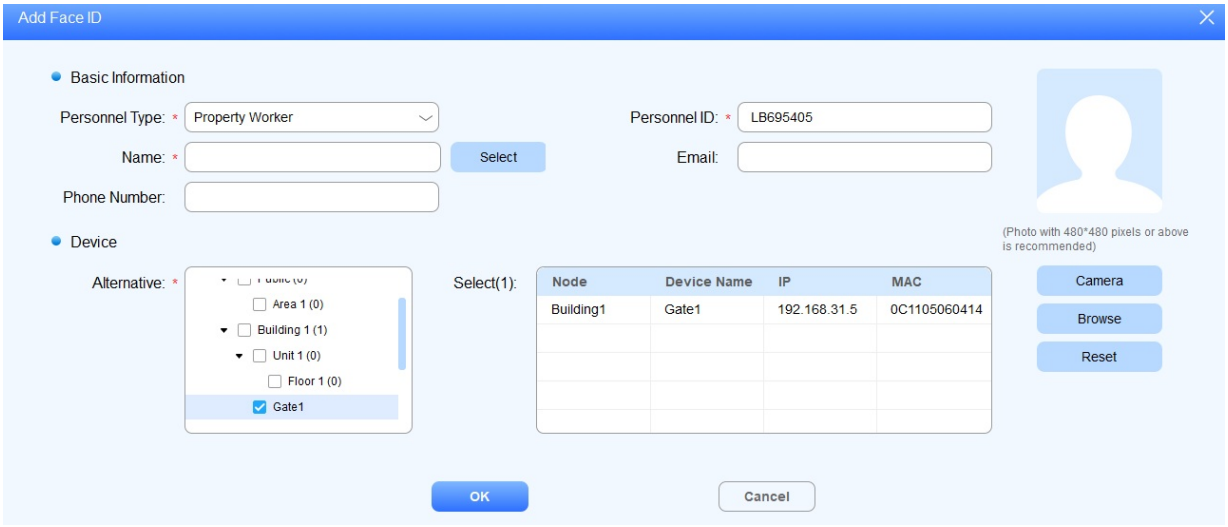
1. Select

   Enter the resident’s name or you can click to select the resident from the existing residents name list, then fill in other information.
2. Select the room node for the resident.(The resident will be able to access the building in which the room is located.)
3. Upload the resident’s picture to SDMC.

- Select **“Property Worker ”** type

1. Select

   Enter the property staff’s name or you can click to select the staff from the existing property staff name list, then fill in other information.
2. Select the specific nodes (locations) where you allow the property staff to gain access to.
3. Upload the property staff ’s picture to SDMC

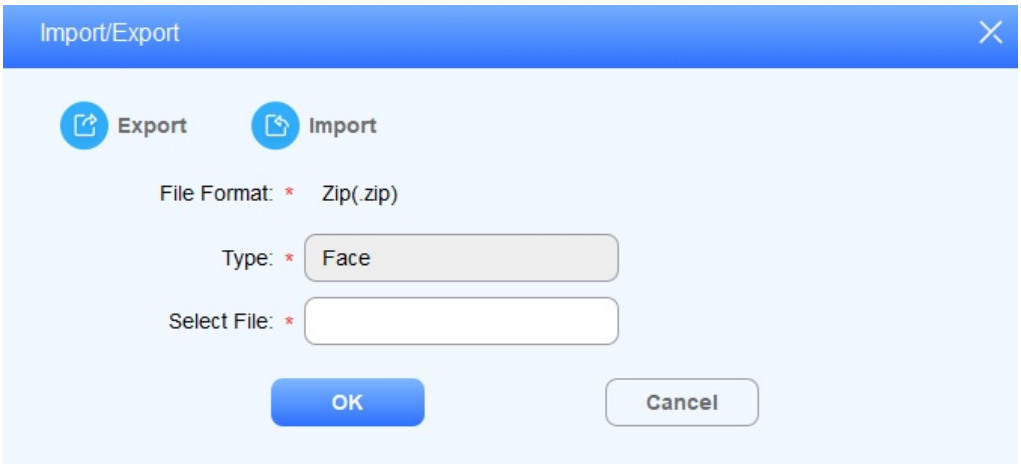


7.4.2.Import/Export Finger Print

You can import face IDs and to SDMC for residents and property staffs for a quicker and larger scale scale face ID enrollment, and export the data out as backup for later user if needed.

1. Navigate to **Personal Management > Verification Mode Manager > Face ID**
2. Click

.



3.Click

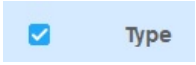
, and select the .zip file, then import the file to the SDMC

4.Click

to export the .zip face data out of the SDMC to your local PC.

7.4.3.Check/Edit/Delete Face Data

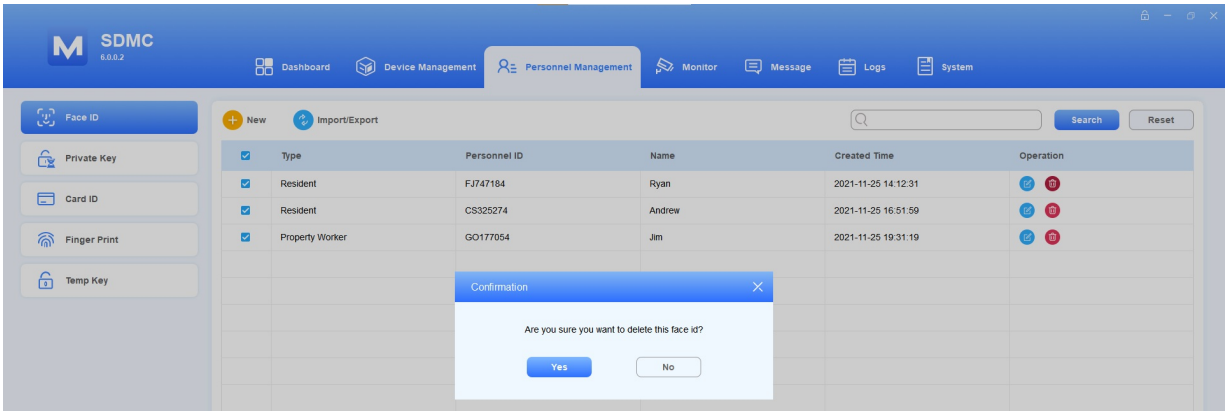
1. Navigate to **Personal Management > Verification Mode Manager > Face ID**
2. Search the face ID by personnel ID, Name in the fuzzy search field. Reset the search keyword if needed.
3. Tick the



checkbox of specific face ID to delete the specific ID or you can tick the to delete all of them.

4. Tick

of the specific resident and property staff for the deletion.



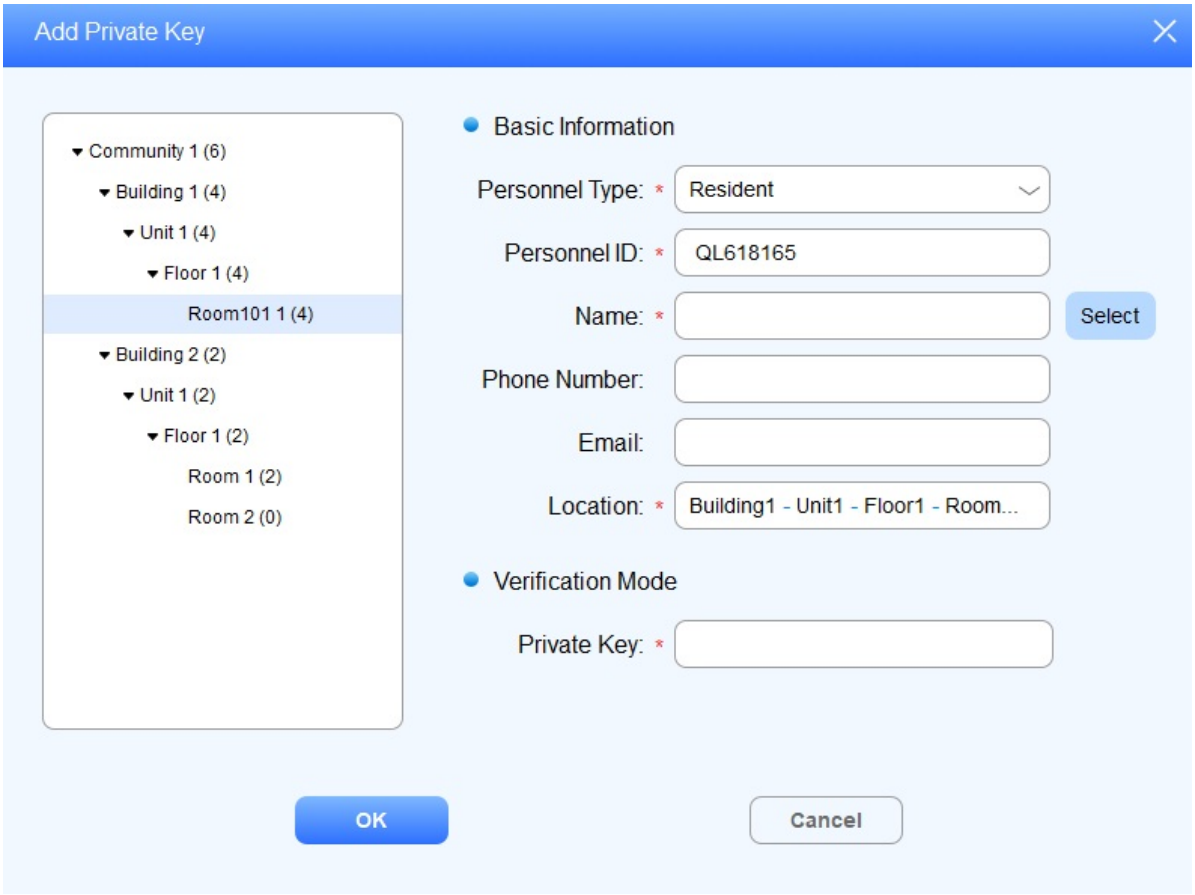
7.5.Private PIN Code

7.5.1.Create Private PIN Code

Private PIN code is used by the residents for door unlock.

1. Navigate to **Personal Management > Verification Mode Manager > Private Key.**
2. Click

3. Select Personnel Type:

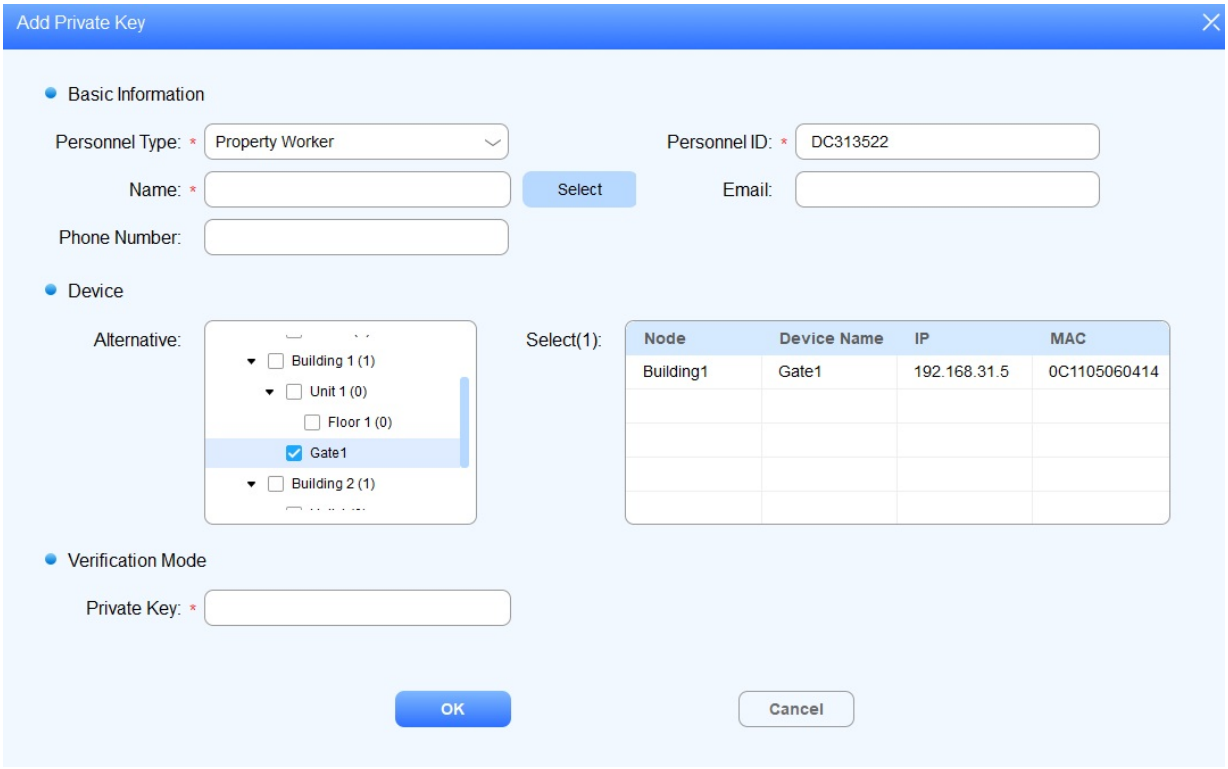


- Select **"Resident"** type

1. Enter the resident's name or you can click
   Select
   to select the resident from the existing residents name list, then fill in other information.
2. Select the room node for the resident.(The resident will be able to access the building in which the room is located.)
3. Create Private PIN code for the resident.

- Select **"Property Worker "** type

1. Enter the property staff's name or you can click
   Select
   to select the staff from the existing property staff name list, then fill in other information.
2. Select the specific nodes (locations) where you allow the property staff to gain access to.
3. Create private PIN Code for the residents.

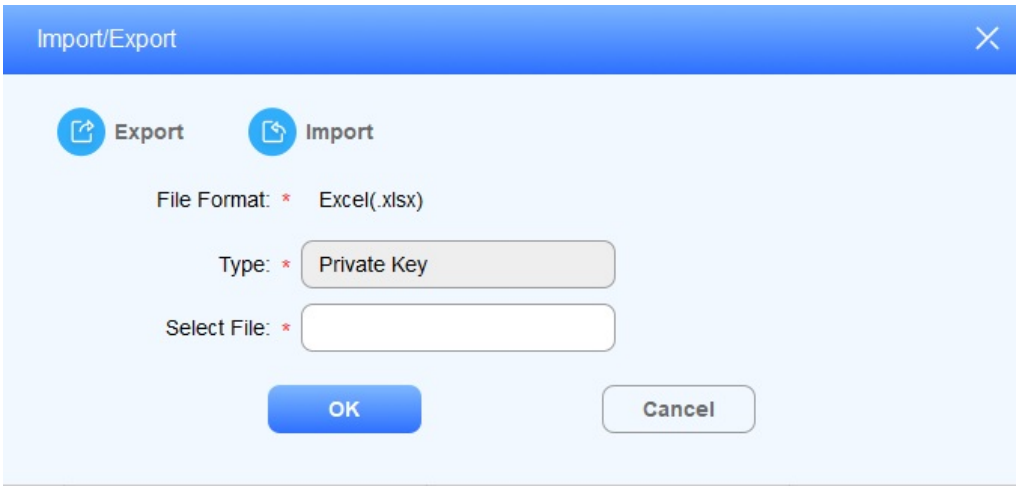


7.5.2.Import/Export Private PIN Code

You can import private PIN code to SDMC for residents for a quicker and larger number of PIN code setup, and export the data out as backup for later user if needed.

1. **Navigate to Personal Management > Verification Mode Manager > Private Key.**
2. Click

.. .



3.Click

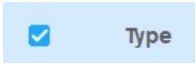
, and select the .zip file, then import the file to the SDMC

4.Click

to export the .zip private PIN code data out of the SDMC to your local PC.

7.5.3.Search/Edit Delete Private PIN Code

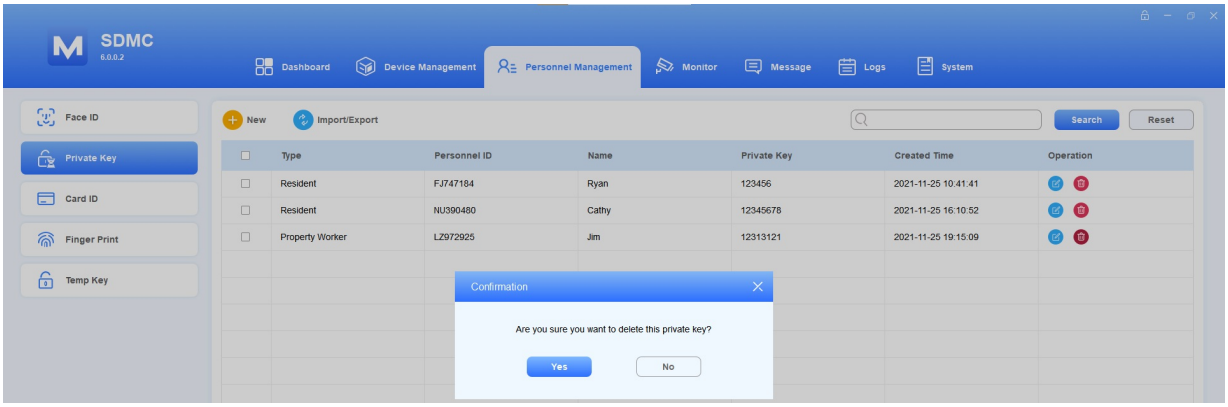
1. Navigate to **Personal Management** > **Verification Mode Manager** > **Private PIN Code**.
2. Search the Private PIN code by **Personnel ID**, **Name** in the fuzzy search field. Reset the search keyword if needed.
3. Tick the checkbox of specific private code for the deletion, or you can tick

   the to delete all of them.
4. Tick

   of the specific resident and property staff for the PIN code deletion.



7.6.Card ID

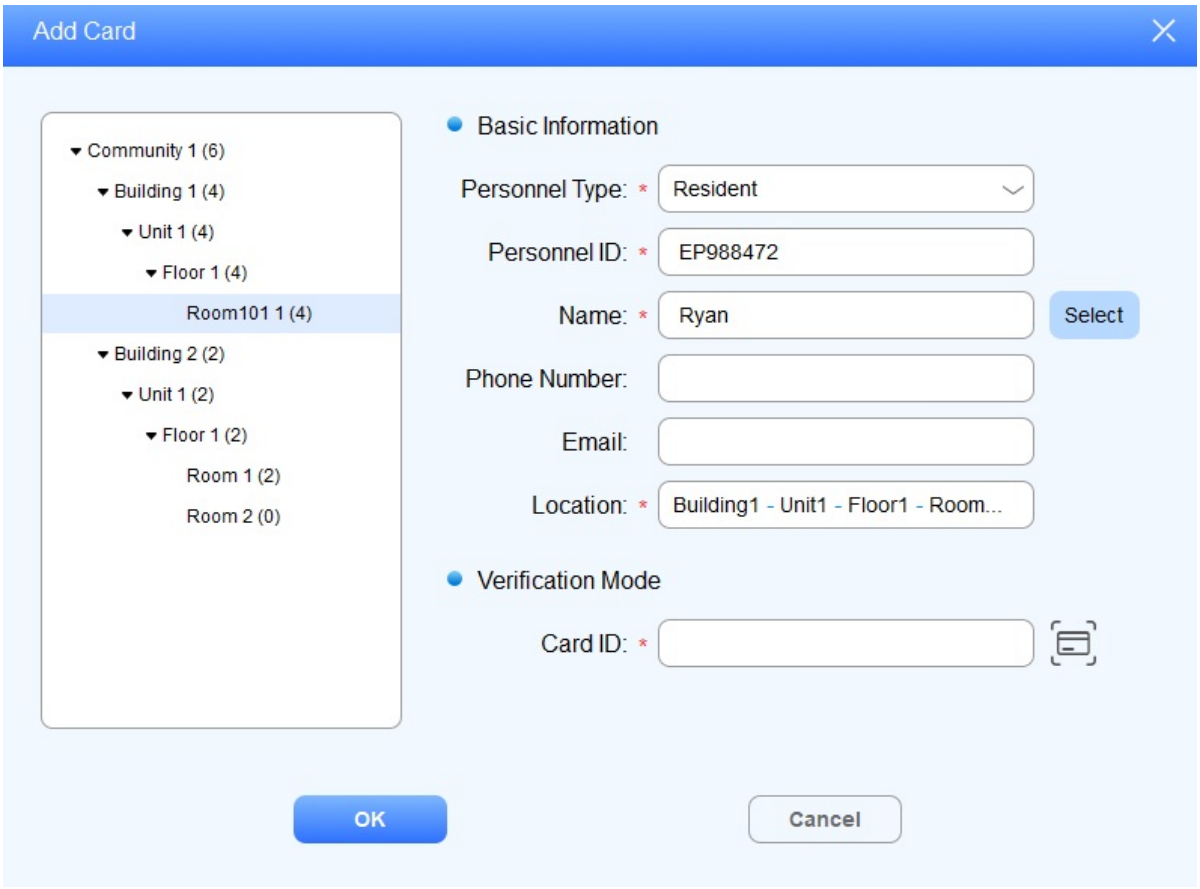
7.6.1.Create Card ID

You can create access card number for both residents and property manager.

1. Navigate to **Personal Management** > **Verification Mode Manager** > **Card ID**.
2. Click

3. Select Personnel Type:

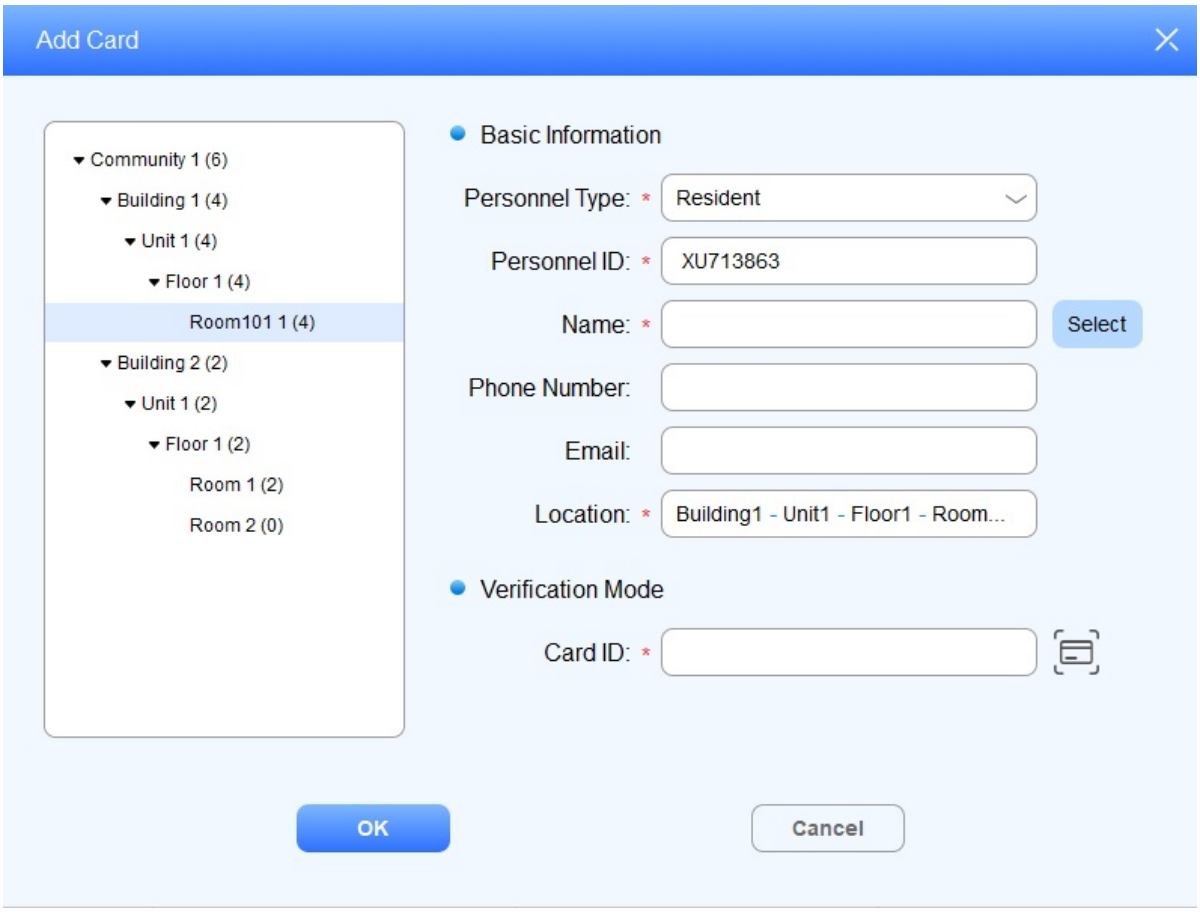


- Select **"Resident"** type

1. Enter the resident's name or you can click
   Select
   to select the resident from the existing residents name list, then fill in other information.
2. Select the room node for the resident.(The resident will be able to access the building in which the room is located.)
3. Click
   to obtain the card number for the card reader, or you fill in the card number manually.

- Select **"Property Worker "** type

1. Enter the staff's name or you can click
   Select
   to select the resident from the existing property stuff's name list, then fill in other information.
2. Select the specific nodes (locations) where you allow the property staff to gain access to.
3. Click
   to obtain the card number for the card reader, or you fill in the card number manually.

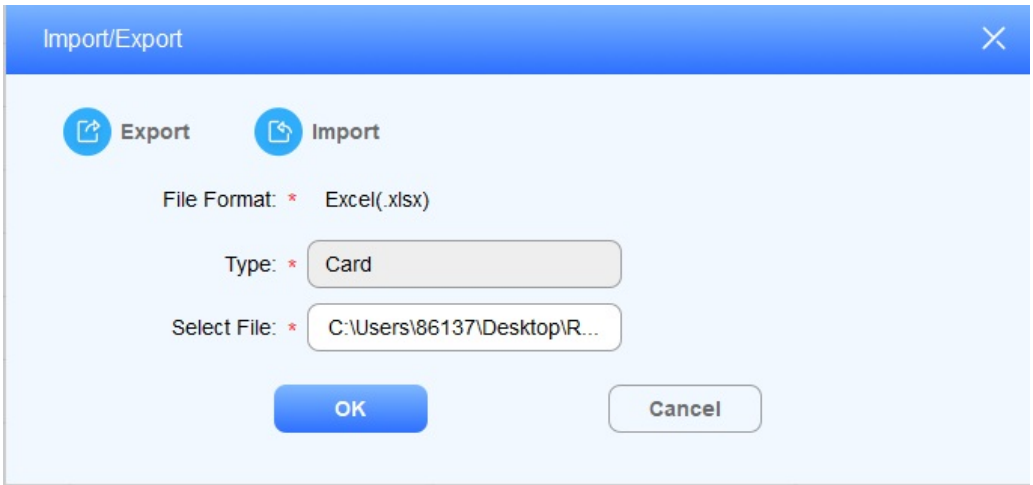


7.6.2.Import/Export Card ID

You can import access card number for residents and property staffs in batch, and export the data out to your local PC as backup for later user if needed.

1. Navigate to **Personal Management** > **Verification Mode Manager** > **Card ID**.
2. Click .

. .



3.Click

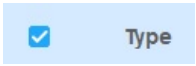
, and select the .xlsx file, then import the file to the SDMC.

4.Click

to export the .xlsx card data out of the SDMC to your local PC.

7.6.3.Search/Edit Delete Card ID

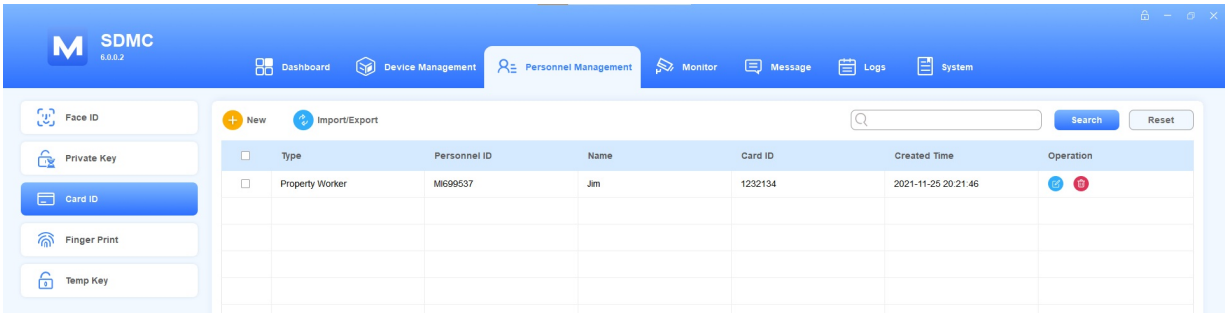
1. Navigate to **Personal Management** > **Verification Mode Manager** > **Face Card ID**
2. Search the face ID by **Personnel ID**, **Name** in the fuzzy search field. Reset the search keyword if needed.
3. Tick the checkbox of specific card ID for the deletion, or you can tick

   the to delete all of them.
4. Tick

   of the specific property staff for the card ID deletion.



7.7.Finger Print

7.7.1.Enroll Finger Print

1. Navigate to **Personal Management** > **Verification Mode Manager** > **Finger Print**
2. Click

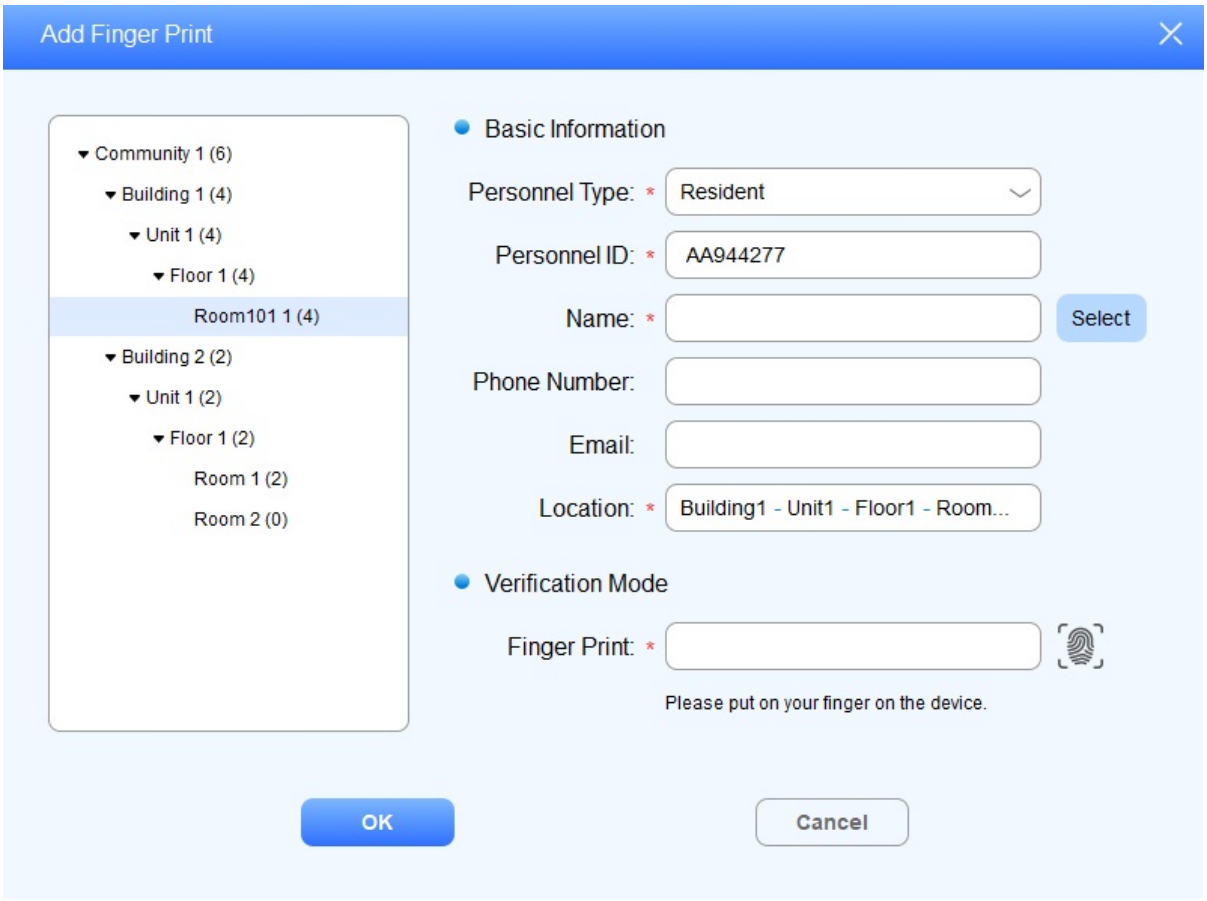
   

3. Select Personnel Type:

- Select **“Resident”** type

1. Enter the resident's name or you can select the resident from the existing residents name list, then fill in other information.
2. Select the room node for the resident.(The resident will be able to access the building in which the room is located.)
3. Click

   to enter the obtained the card number from the card reader, or you can fill in the card number.



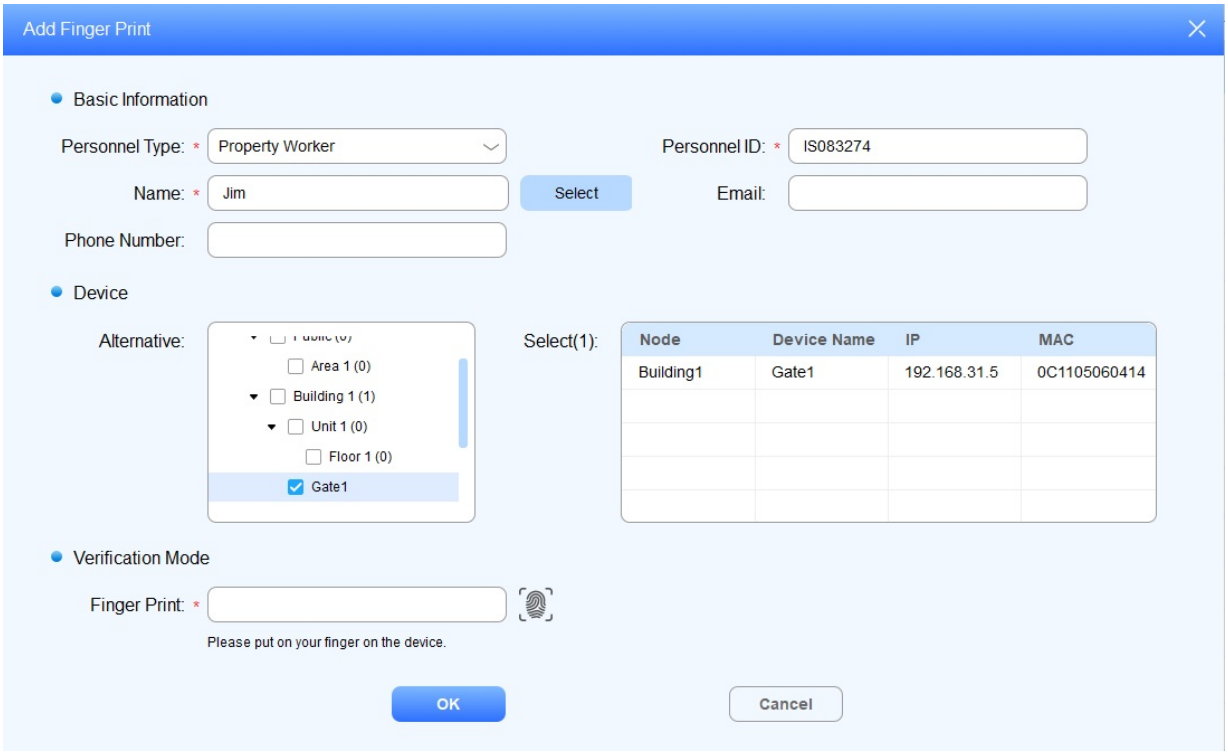
- Select "**Property Worker** " type

1. Enter the property staff's name or you can click

   Select

   to select the staff from the existing property staff name list, then fill in other information.
2. Select the specific nodes (locations) where you allow the property staff to gain access to.
3. Click

   to enroll finger data for the property staff.

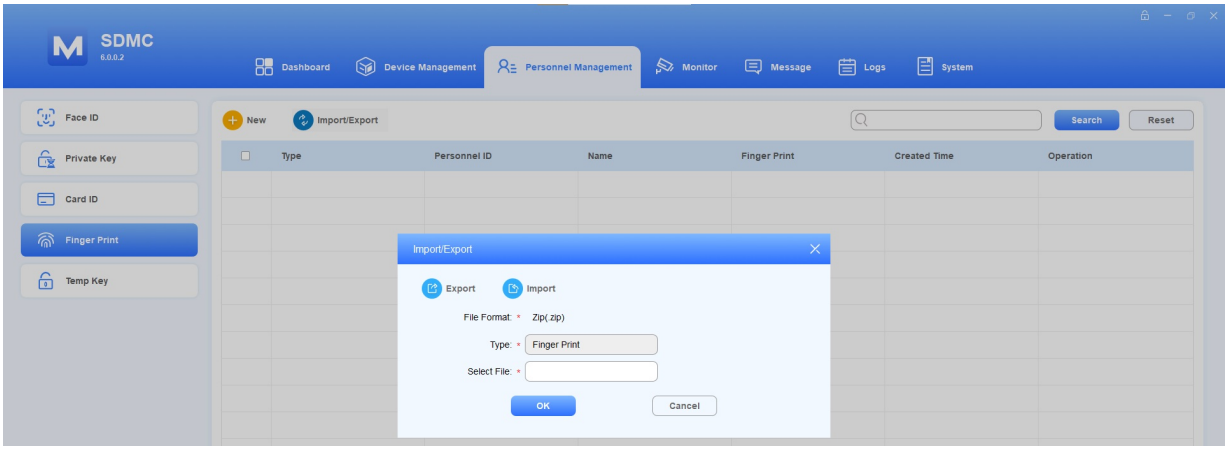


7.7.2.Import/Export Finger Print

You can import finger print data to SDMC for residents and property staffs for a quicker and larger scale scale finger print enrollment, and export the data out as backup for later user if needed.

1. Navigate to **Personal Management** > **Verification Mode Manager** > **Finger Print**
2. Click .

. .



3.Click

, and select the .zip file, then import the file to the SDMC

4.Click

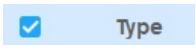
to export the .zip finger print data out of the SDMC to your local PC.

7.7.3.Check/Edit/Delete Finger Print Data

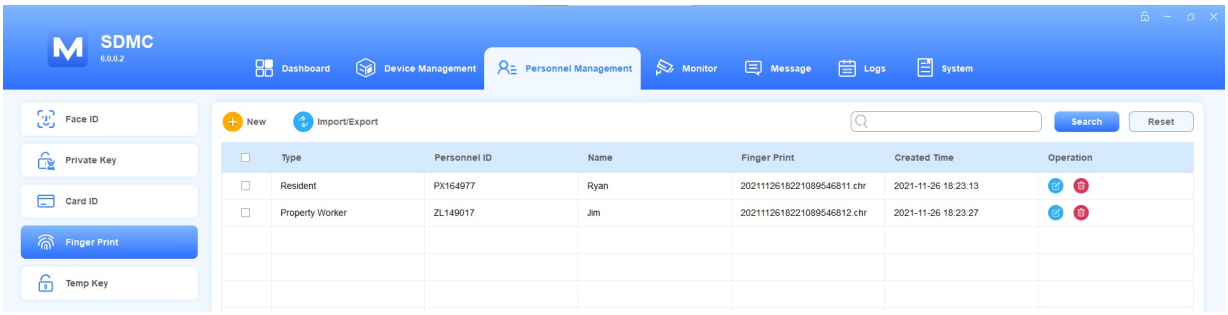
1. Navigate to **Personal Management** > **Verification Mode Manager** > **Finger Print**.
2. Search the finger print data in the fuzzy search field by **Personnel ID**, **Name** and **Finger Print** code .
3. Click

   of the specific finger print for deletion or tick

   to delete all the finger print if needed.

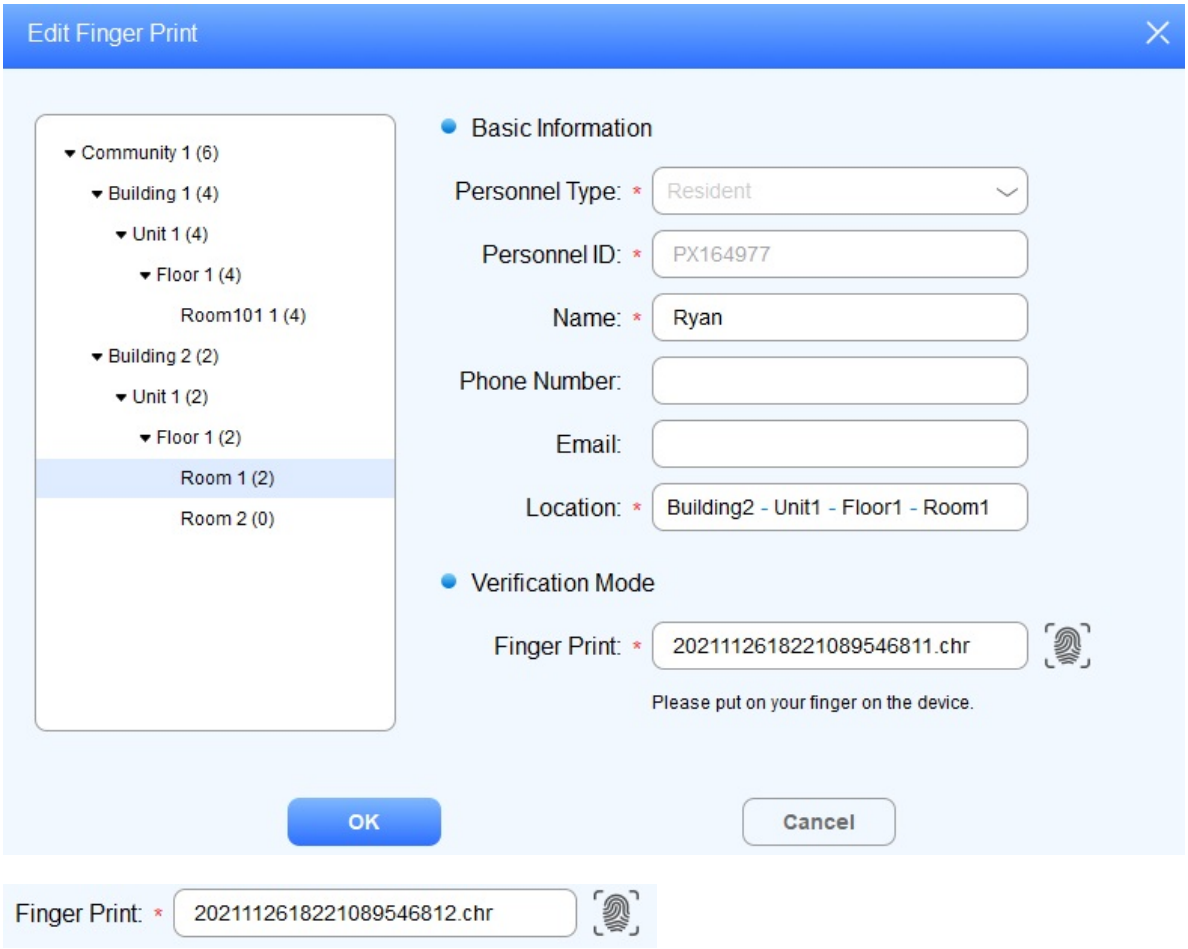


4.Click

of the specific finger, and edit the finger print.

- **Edit Finger print for Resident**

1. Edit the resident finger print information.
2. Change the room node to which the finger print access method is to be applied by the resident.

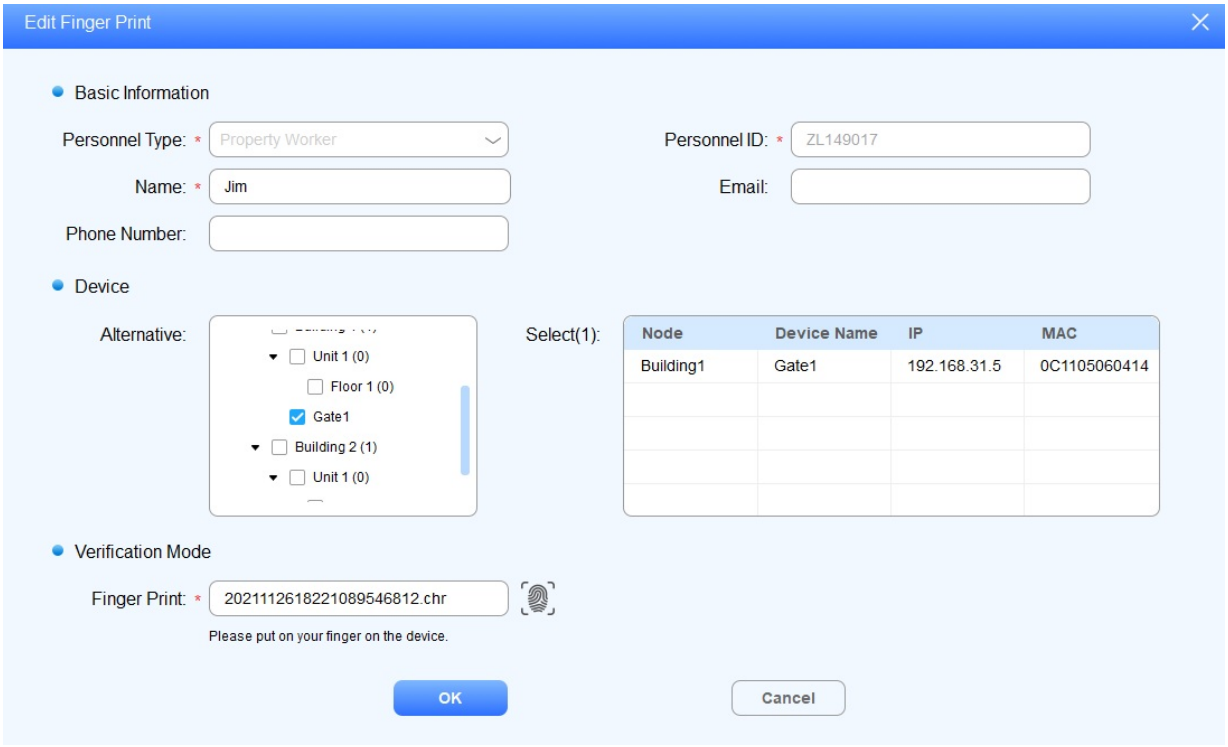


Note:

Do not change the finer print code. eg . If change, it will result in invalid finger print authentication.

- **Edit Finger print for Property Manager**

1. Edit the resident finger print information.
2. Change the node to which the finger print access method is to be applied by the property staff.



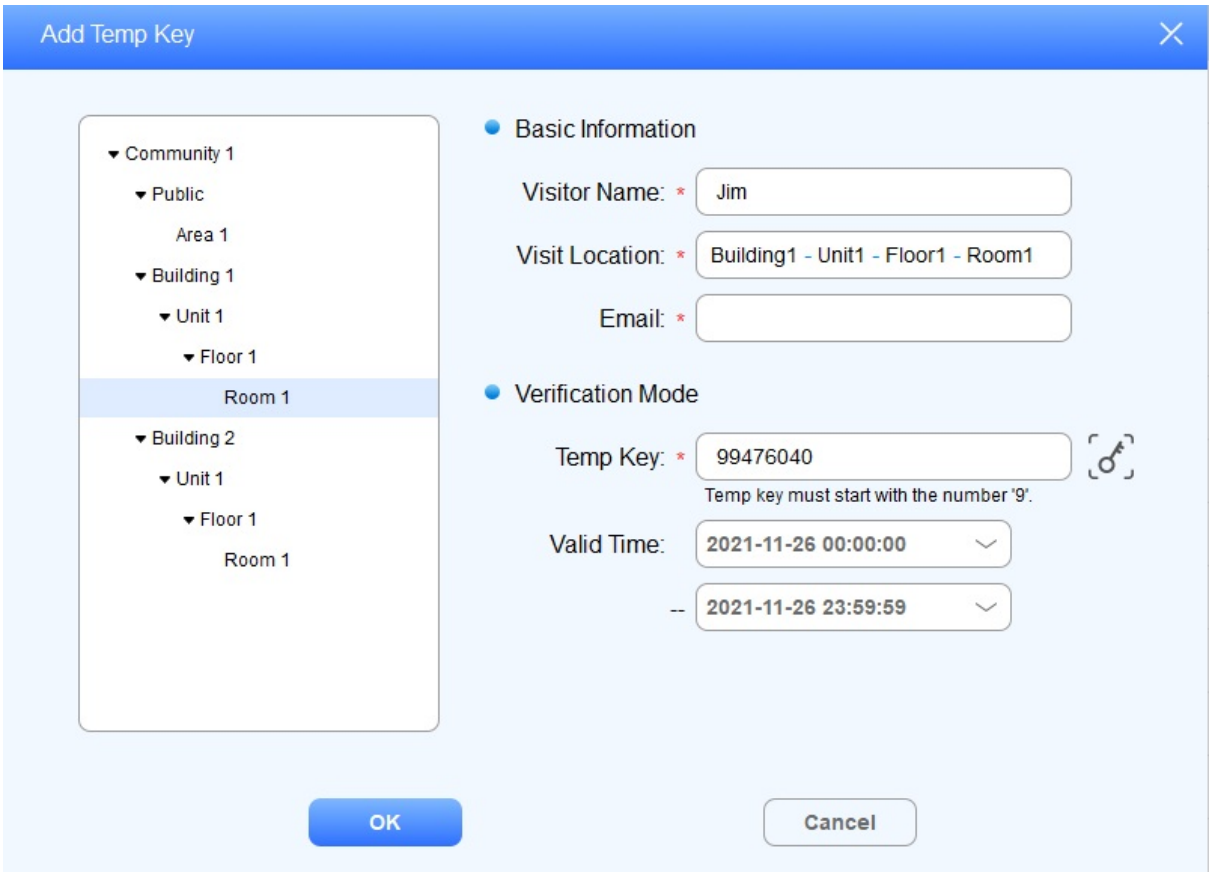
7.8.Temporary PIN Code

7.8.1.Create Temporary PIN Code

You can generate temporary PIN code with validity time range for the visitors to access the location you selected.

1. Navigate to **Personal Management** > **Verification Mode Manager** > **Temp Key**
2. Click
   

3. Enter the visitor's name, and select the visitor's visiting location that you allow the visitor to gain access to.
4. Enter the visitor's email for receiving temporary PIN code.
5. Click
   
   to generate temporary PIN code for the visitor, or enter the PIN code manually.
6. Set the PIN code validity time range, then press **Okay** for the confirmation



- **Field Name Description**

NO.	Field Name	Description
1	Visitor Name	Enter the visitor name, which should be 63 digits maximum in length. The visitor's name can be seen in the access log.
2	Visitor Location	Select the location (node) that you allow the visitor to access to. The node you selected can be applicable upwards. For example if you select the node "Building1" then the visitor is also allowed to access the "Community1" node, which is above the Building node.
3	Email	Email should be 255 digits in length maximum.
6	TempKey	Temporary PIN code should be 2-8 digit numbers starting with the number 9. You can change the PIN code after its being generated.
	Valid Time	Set the validity time range for the temporary PIN code. The default valid time range is "00:00:00-23:59:59" of the day.

7.8.2.Check/ Edit /Delete Temporary PIN Code

After the Temporary PIN code is generated, you can change the visitor's information in terms of their names, visiting location, emails, and temporary PIN code along with its validity time range if needed.

1. Navigate to **Personal Management** > **Verification Mode Manager** > **Temp Key**.
2. Search the temporary PIN code in the search field by **Personnel ID**, **Name** and temporary PIN code .
3. Click

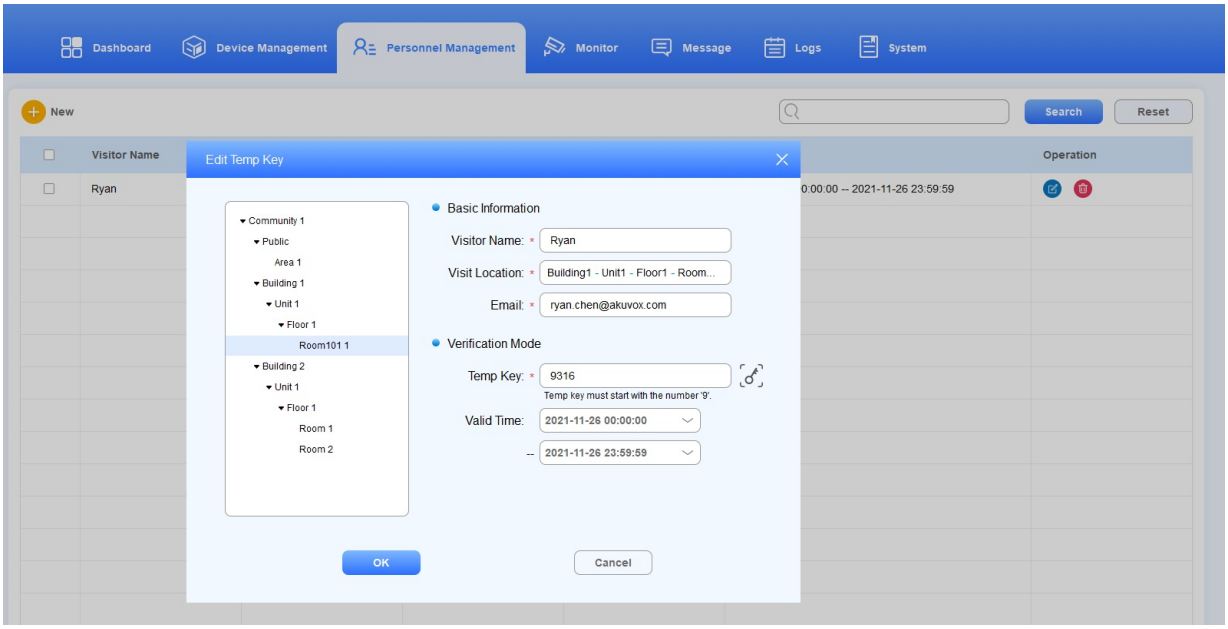
   of the specific temporary PIN code for deletion or tick

   Type

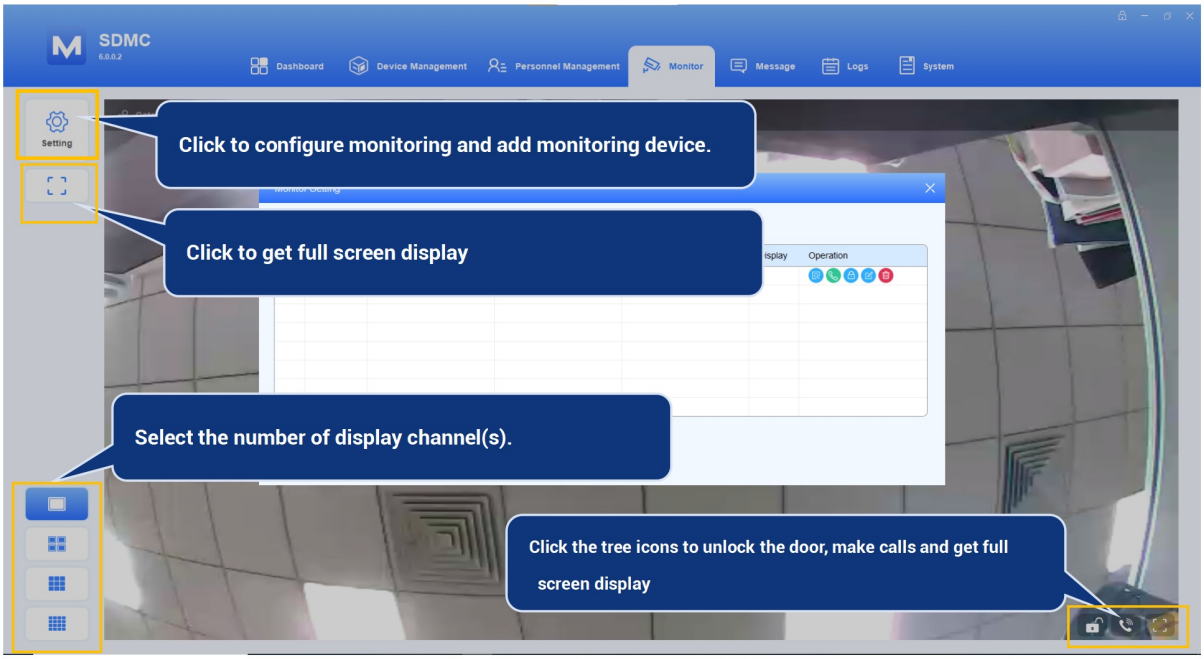
   to delete all the temporary PIN code if needed.
4. Tick the checkbox of the visitor and edit temporary PIN code information if needed.
5. Tick the check box of the visitor(s) or tick

   Visitor Name

   to delete all the Temporary PIN code if needed.



8.Monitor

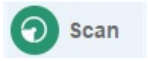


8.1.Setting

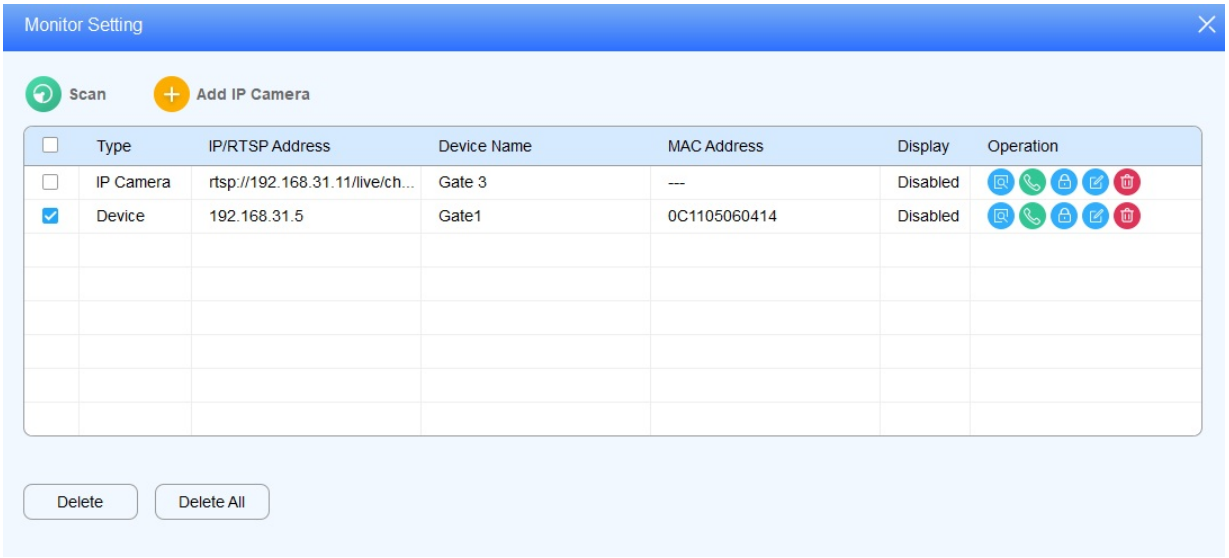
8.1.1.Add Monitoring Device

You can add Akuvox door phones as monitoring devices in the same LAN network via scanning and you can also add third party IP camera for monitoring if needed.

- **Add Akuvox Door Phone via Scanning**

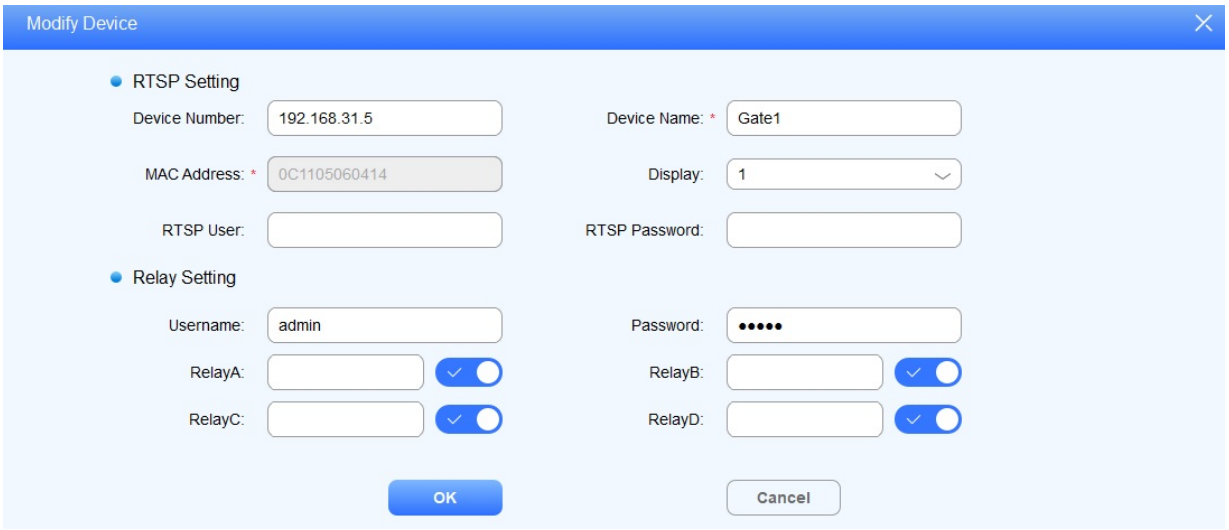
1. Click
   
   and click
   

   .
2. Tick the checkbox of the door phone you want to add, then click
   
   .



3.Enter the RTSP username and password for authentication, and select the number of the channel display.

4.Enter the relay username and password for authentication,and enable relay(s) as needed.



- **Field Name Description:**

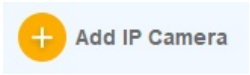
NO.	Field Name	Descriptions
1	Device number	Shows the monitoring device IP address.
2	Device Name	Shows the monitoring device name by location.
3	MAC Address	Shows the monitoring device MAC address.
4	Display	Select the number of channel if you want to view the monitoring video (from 1 -16 channels).
5	RTSP User	Enter the door phone RTSP username for authentication.
6	RTSP Password	Enter the door phone RTSP password for authentication.
7	Username	Enter the door phone relay username for authentication.

8	Password	Enter the door phone password for authentication.
9	Relay A/B/C/D	Enable the relay(s) that can be triggered while you are monitoring.

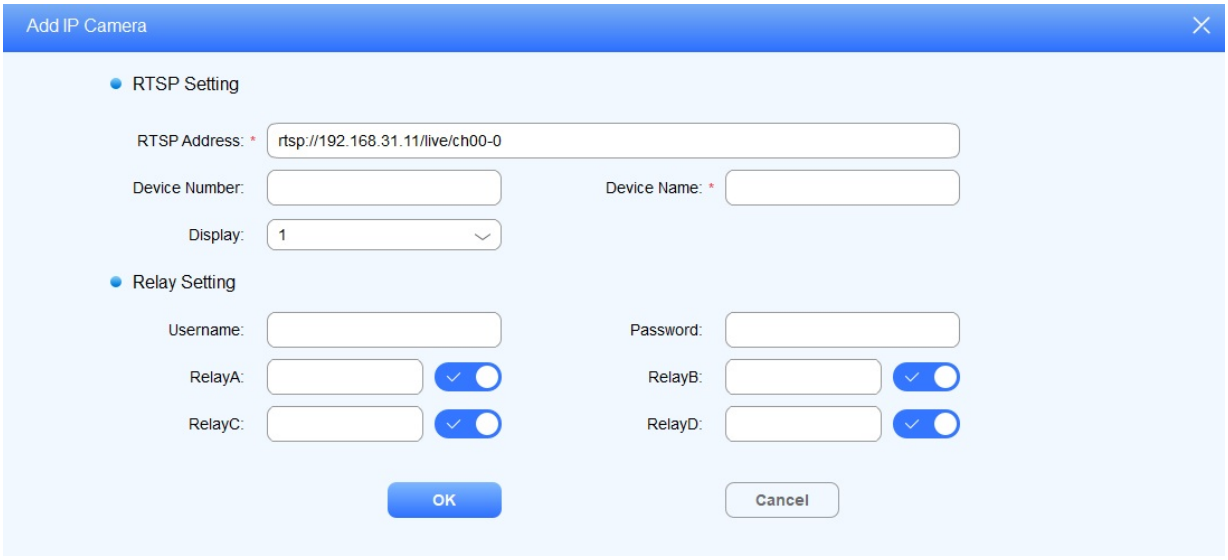
Note:

- The number of channel selected should be matched with channel display icon you selected. For example, if you select “5” for the channel display, and you select  , then the video will not displayed, you instead, should select the channel icon greater than 5.

- **Add Third Party IP camera**

1. Click  , then click 

2. Fill in the RTSP URL of the IP camera.
3. Fill the IP address of the access-controlling door phone.
4. Enter device name of the IP camera, and select the number of display channel.
5. Enter the relay username and password for the authentication.
6. Enable the relay(s) as needed.



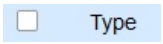
- **Field Name Description:**

NO.	Field Name	Descriptions
1	RTSP Address	Enter the RTSP address in the URL format provided by third party IP camera.
2	Device Name	Enter the IP address of the door phone that trigger the relay for the door unlock.
3	MAC Address	Enter the IP camera name, for example by its location.
4	Device Number	Enter the IP address of the door phone that is located closer to the the IP camera.

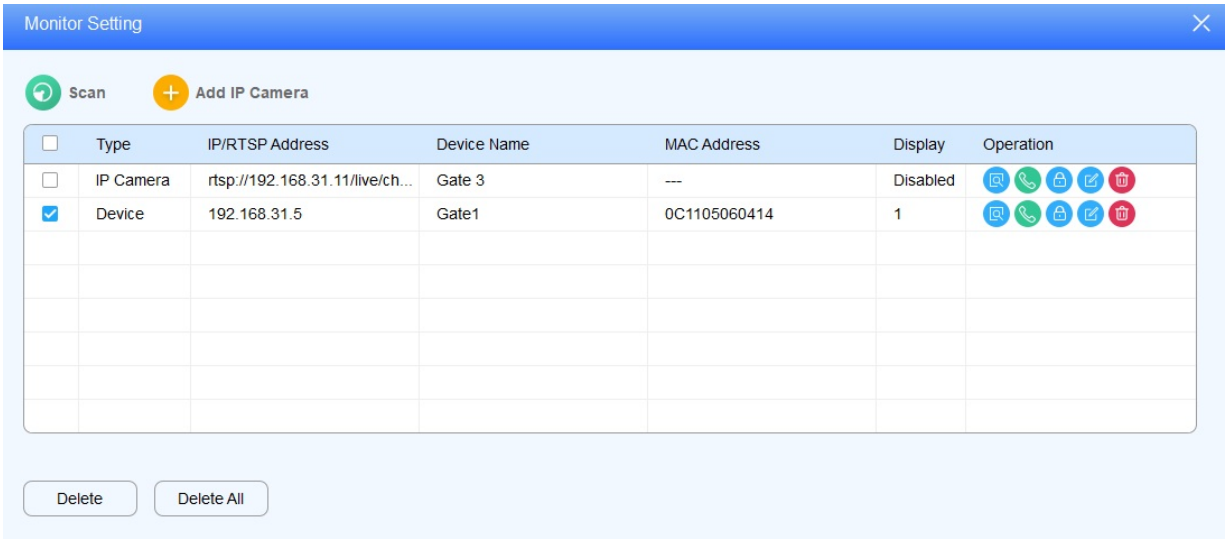
8.1.2.Edit/Delete Monitoring Device

You can edit and delete the monitoring device if needed.

1. Click 

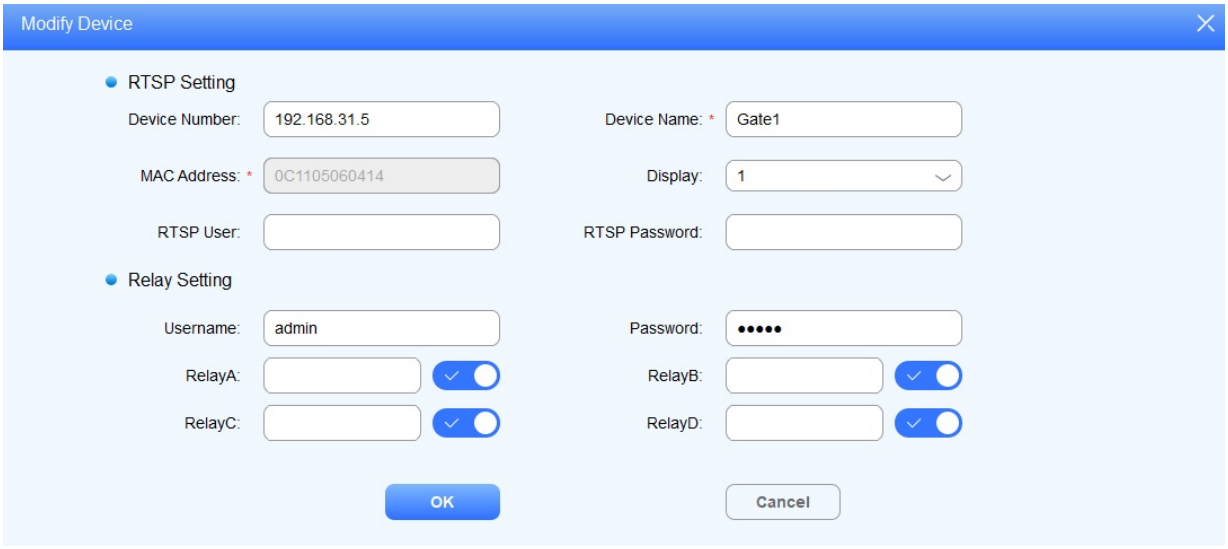
   of specific monitoring device you want to delete, or tic 

   k to delete all the monitoring device.



2.Click 

to edit RTSP setting and relay setting if needed.



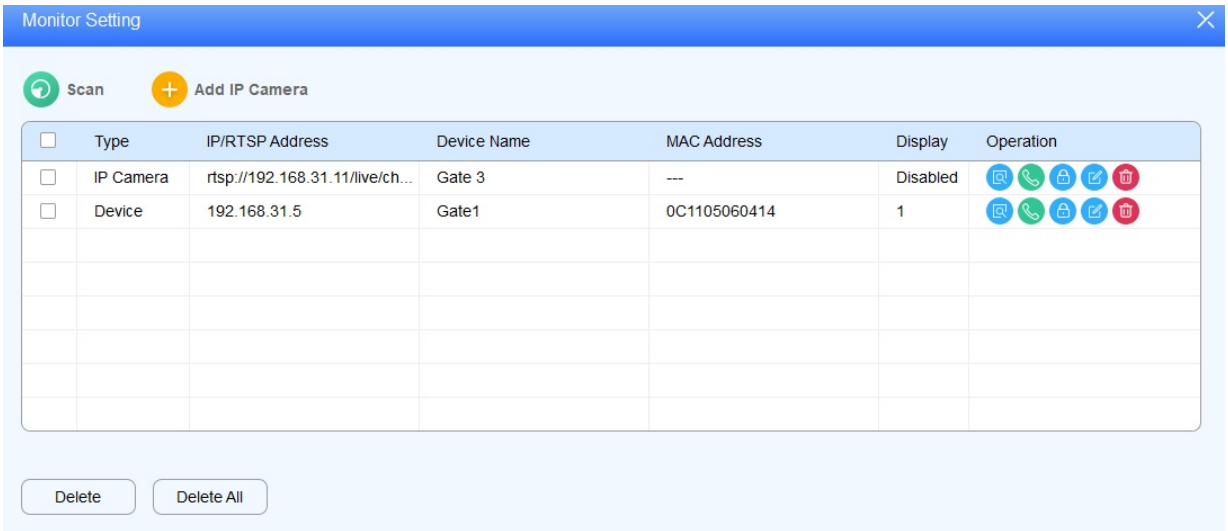
8.1.3. Preview/Call/Unlock

After the monitoring device is set up, you can preview the video image from monitoring device to see who is standing at the door station, while making call to the person before you unlock the door.

1. Click

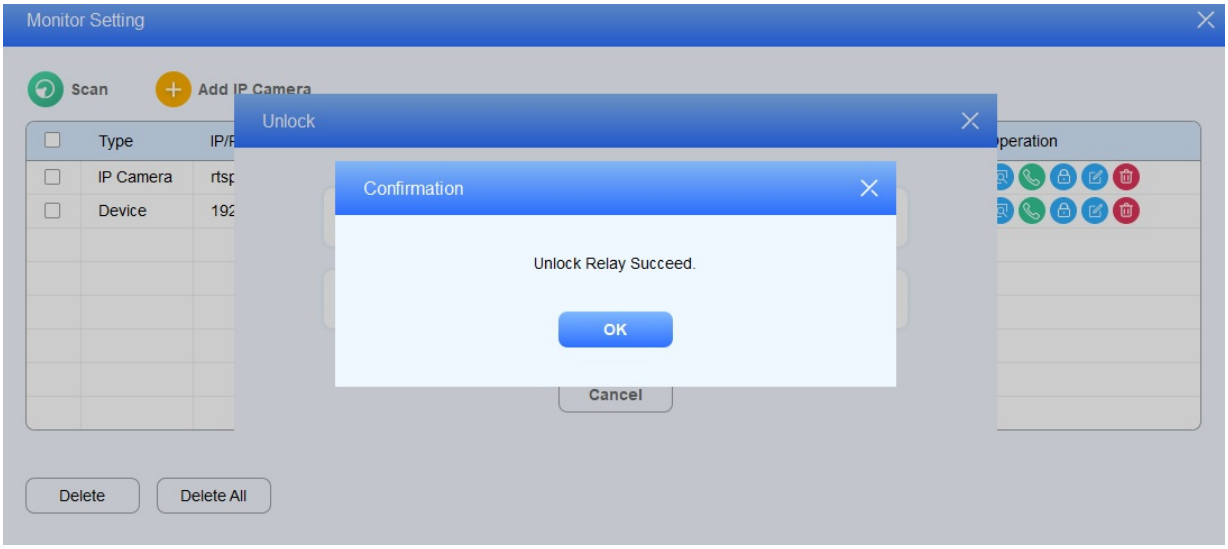
   of the monitoring device want to take a preview of the video image.
2. Click on

   to call the monitoring device if needed



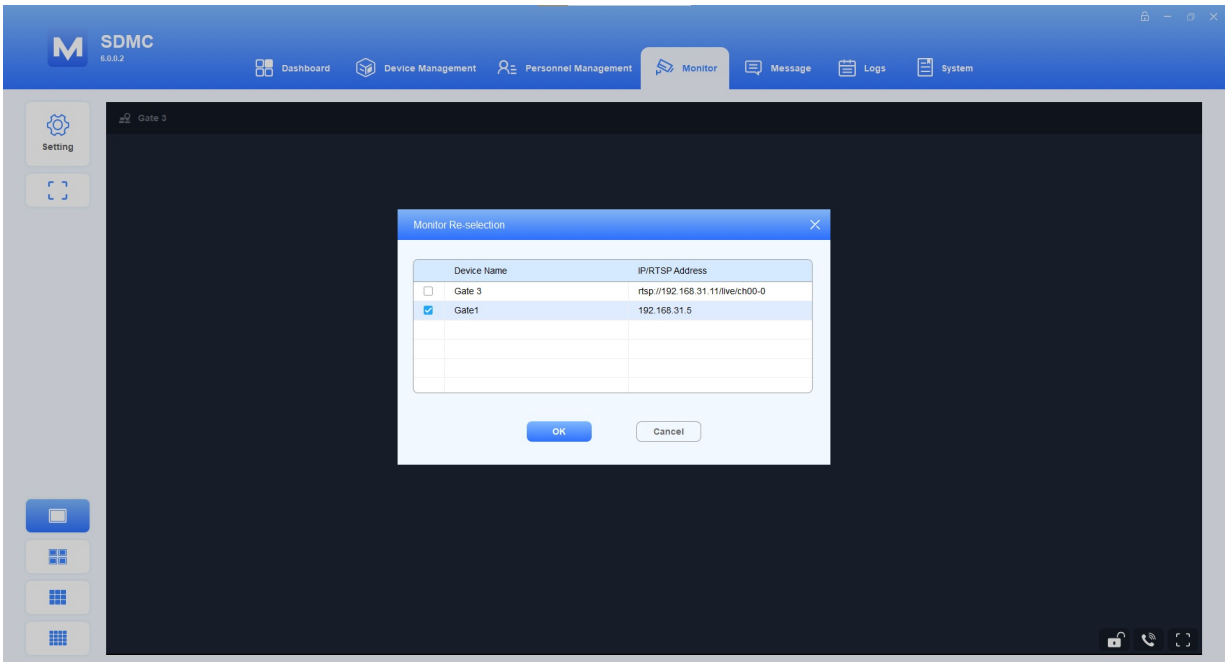
Click

to unlock the access-controlling door phone.



In addition, you can take a quick view of the full screen video footage from the monitoring device you want to monitor.

1. Click on the upper area as high-lighted in yellow.
2. Select the monitoring devices you want to monitor.

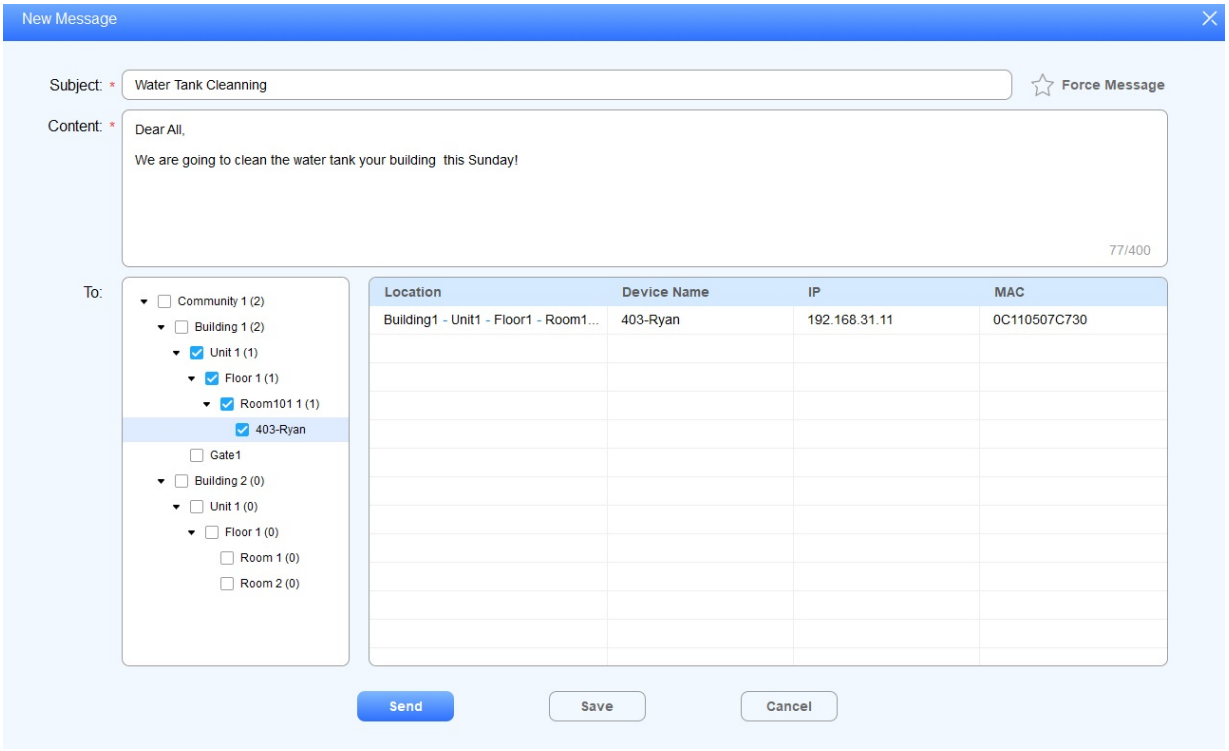


9.Message

9.1.Create /Draft/ Send Message

You can Create, draft, send, messages or notifications to the targeted residents or to all the residents in the community if needed.

1. Click **Message** module, and select **Text Message**.
2. Create the subject and the message, then select the specific residents (by their room node(s))
3. Click **Send** to send message to the device (eg indoor monitor) you selected, or you can click **Save** to save the message as a draft for later used if needed.



9.2. Import/Export Message

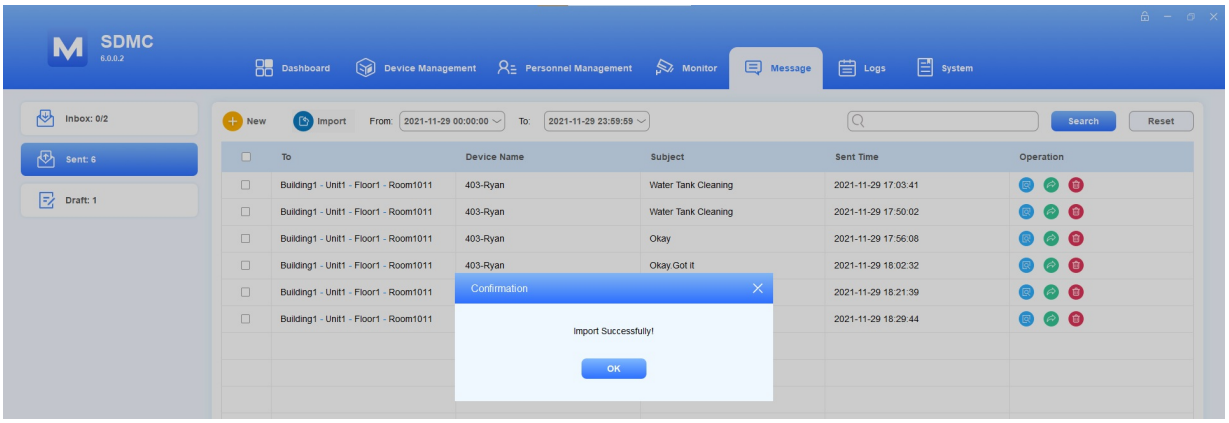
You can import the message template file from your local PC to SDMC, and the message in the file will be automatically sent to the designated device node. You can export the received messages if needed.

- **Import/Send Message to Residents**

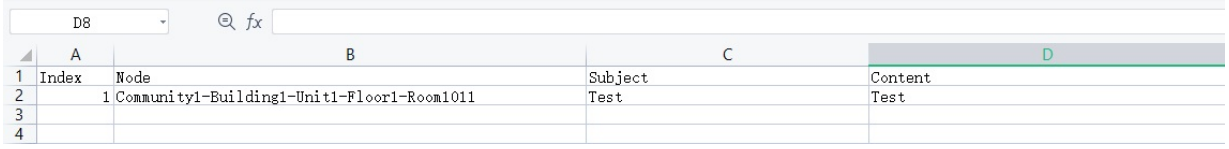
1. Navigate to **Message > Text Message > Sent**.
2. Click

   Import

   to select the .xlsx message file from your local PC, and import the message file to the SDMC, which will send the message to the specific device node.



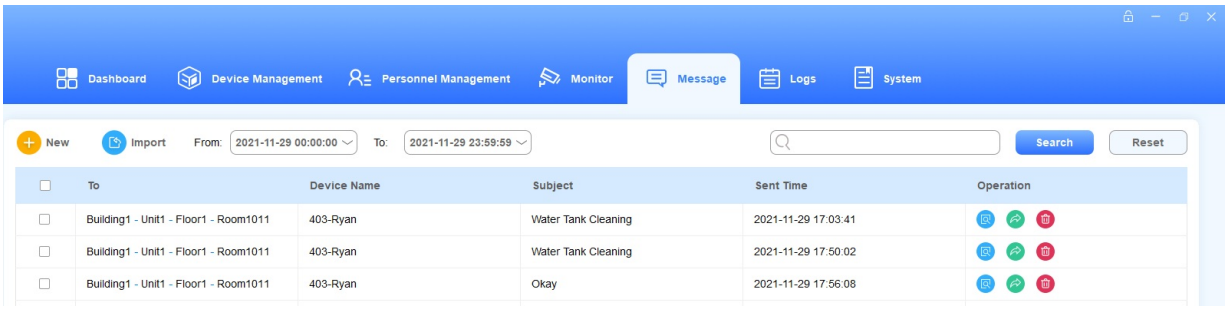
- **Import Template**:



	A	B	C	D
1	Index	Node	Subject	Content
2	1	Community1-Building1-Unit1-Floor1-Room1011	Test	Test
3				
4				

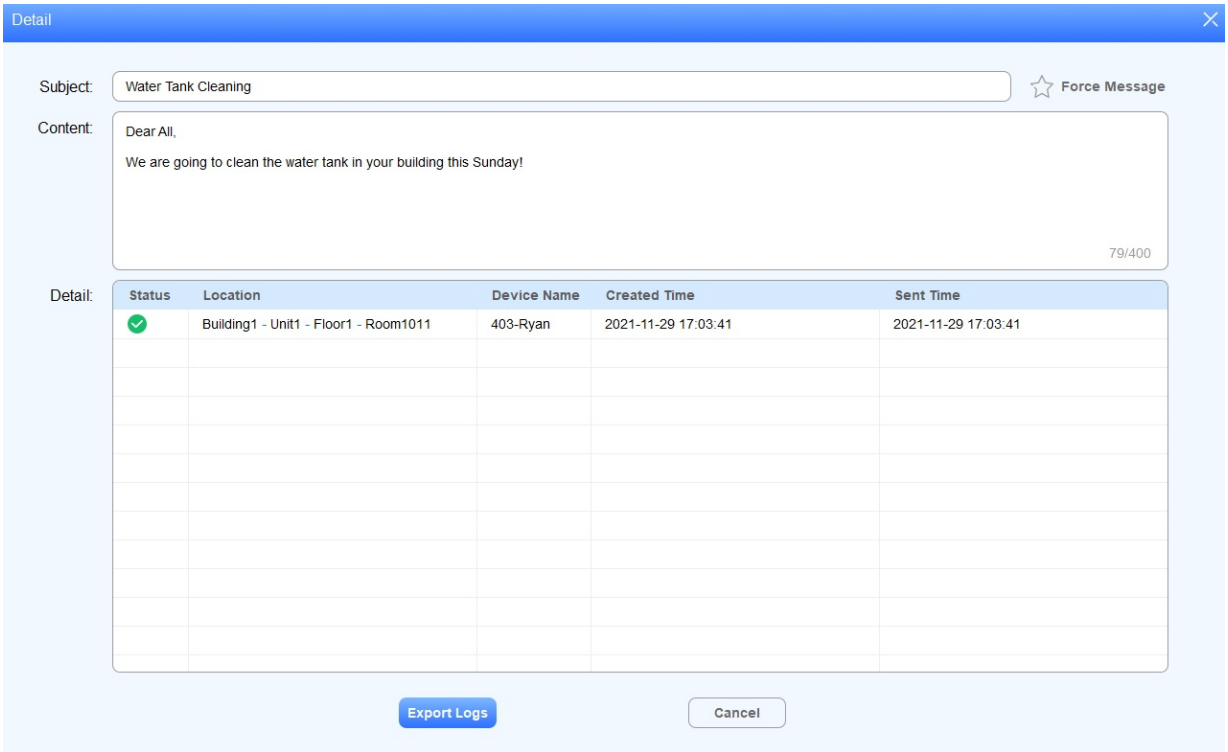
- **Export Message**

1. Click
   
   of the specific message you want to export.



2.Click


to export the message to your local PC.

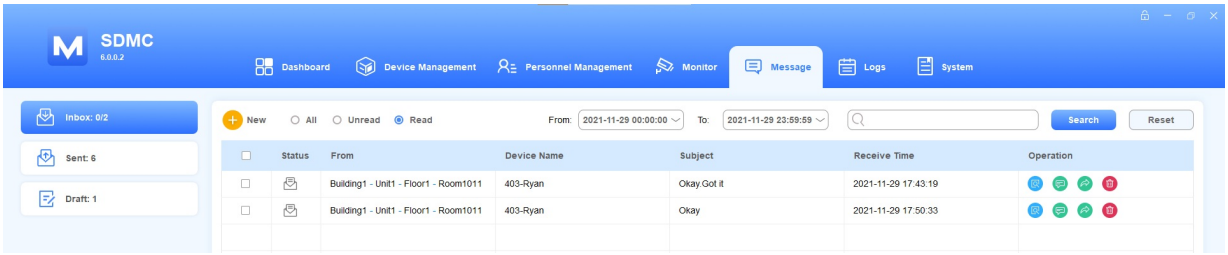


9.2.1.Check/Reply/Forward/Delete/Edit Message

9.2.1.1.Check/ Reply/ Forward/Delete Received Messages

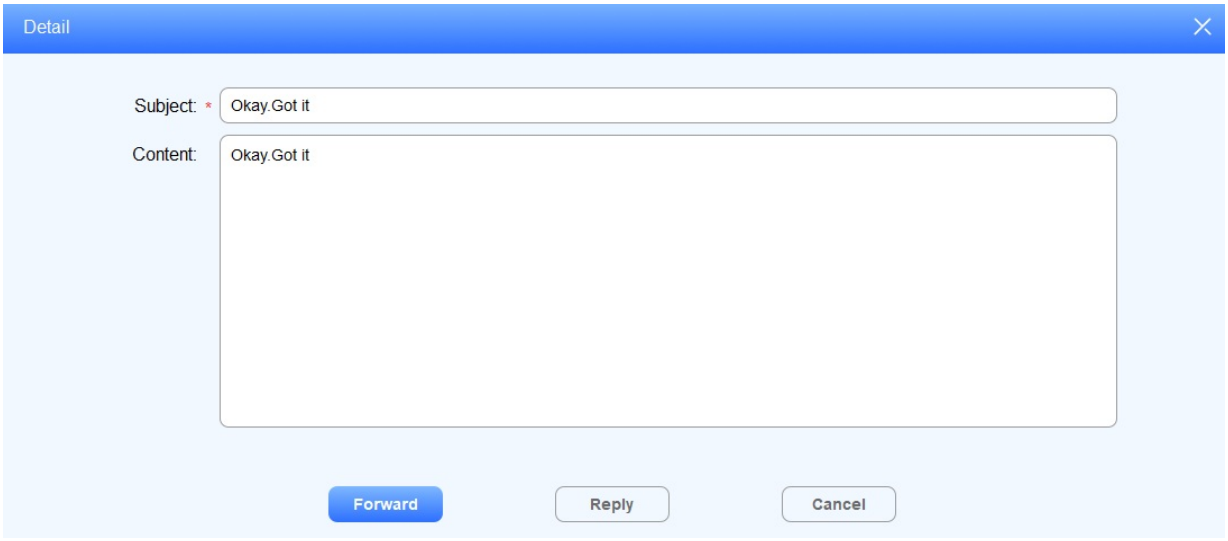
You check, reply, forward, and delete the messages in the inbox.

1. Select **Message > Text Message > Inbox**
2. Search the message by **Date/All/Read/Unread**, or enter the keyword in the fuzzy search field by **Device name**, **Subject**.



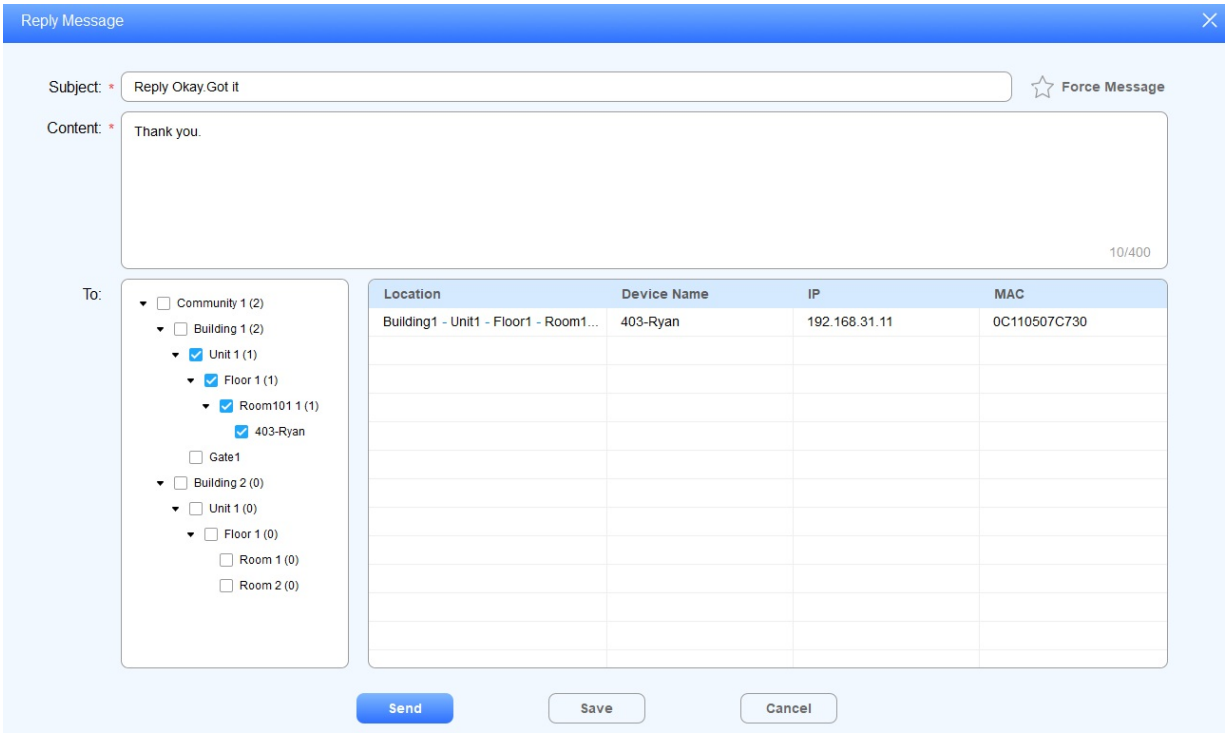
3.Click

of the specific received message you want to check. You can also forward or reply the message while you are checking the message for details.



4.Click

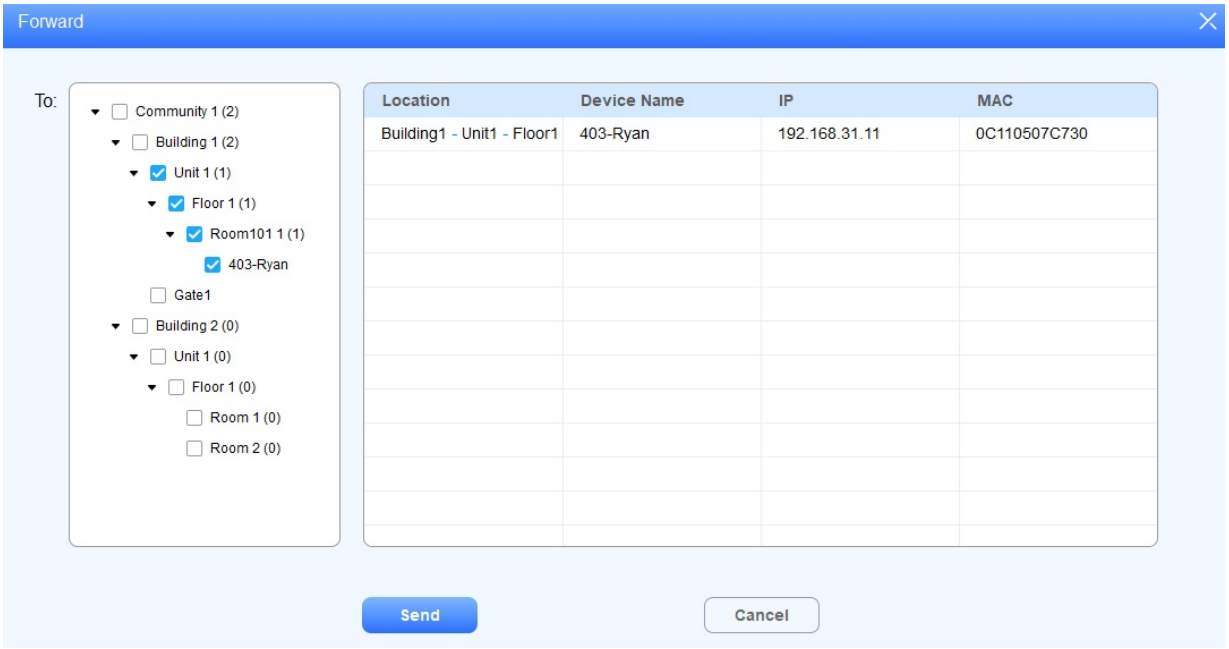
of the specific received message you want to reply, and create you reply message, then click **Send**.



5.Click

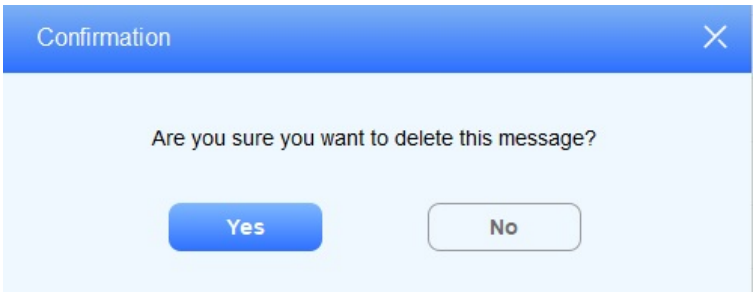
of the specific message you want to forward to other residents.

6.Select the node(s) to which you want to forward the message.



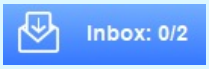
7.Click

the specific received message you want to delete



Note:

The two numbers on both side of "/" indicates the total number of received message and unread messages. For example



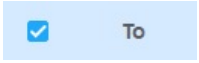
, 2 is total number of messages, 0 is the total number unread message.

9.2.1.2.Check/Forward/Delete Sent Messages

1. Select **Message > Text Message > Sent.**
2. Search the message by **Date**, or enter the keyword in the fuzzy search field by **Device name**, **Subject**.
3. Click

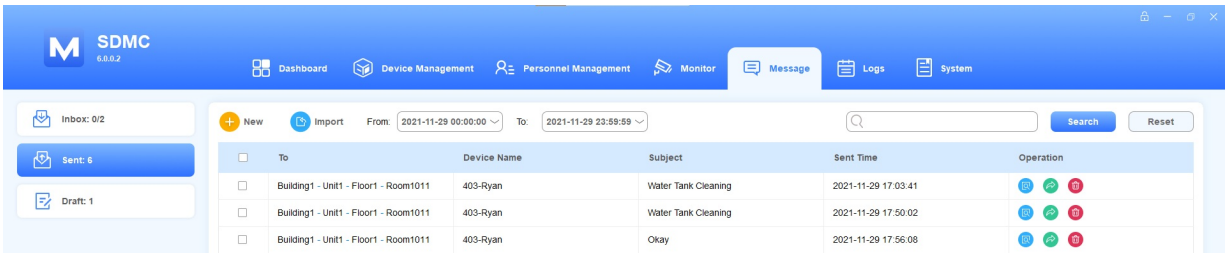
   on of the sent message you want to delete , or tick th

   e to delete all the sent messages.
4. Click

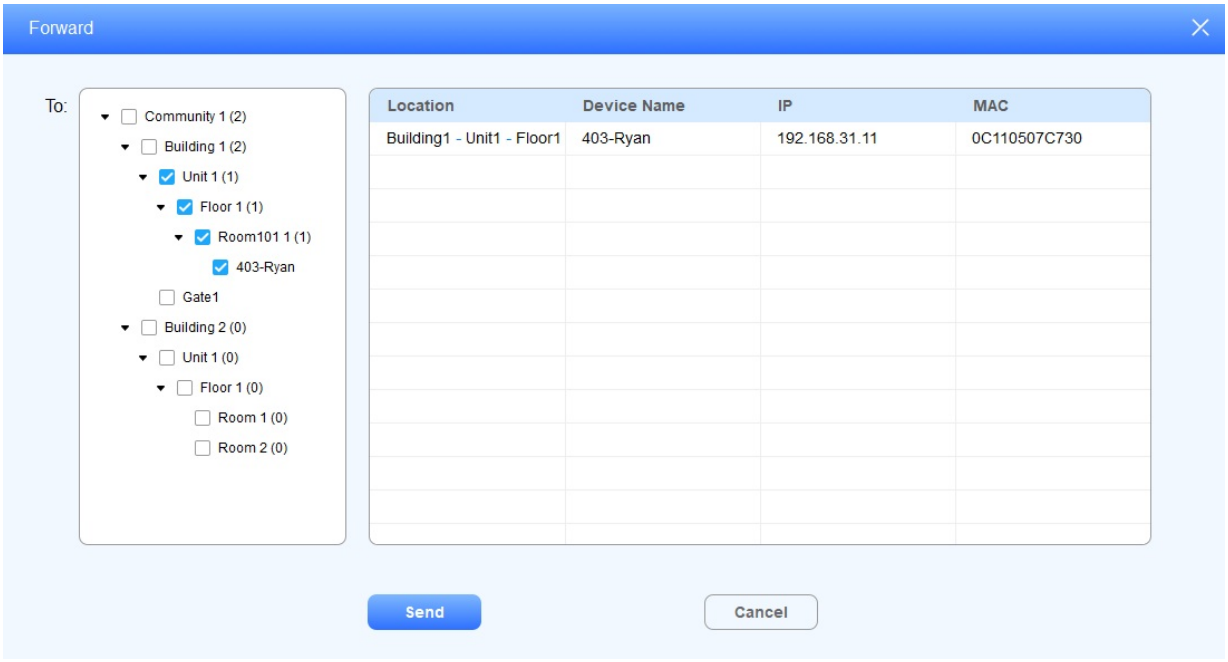
   

   of the specific sent message you want to check.



5.Click

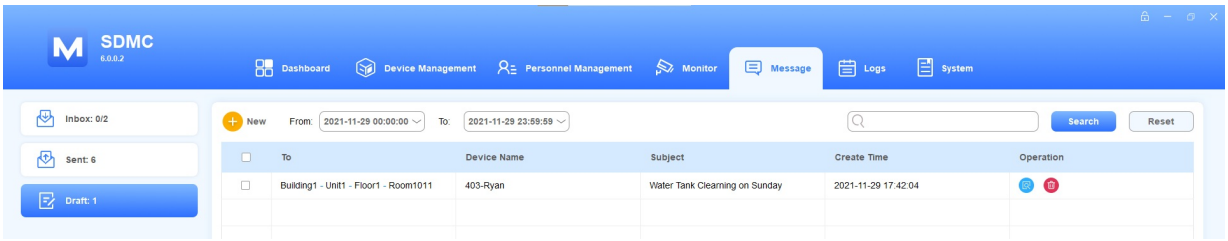
of the specific sent message you want to forward to other residents. Select the node(s) to which you want to send the message .



9.2.1.3. Edit/Delete Draft messages

You can edit the draft message before sending to targeted residents, and delete draft message if needed.

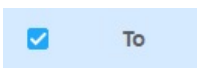
1. Select **Message > Text Message > Draft**.
2. Search the message by **Date**, or enter the keyword in the fuzzy search field by **Device name**, **Subject**.



1. Click on

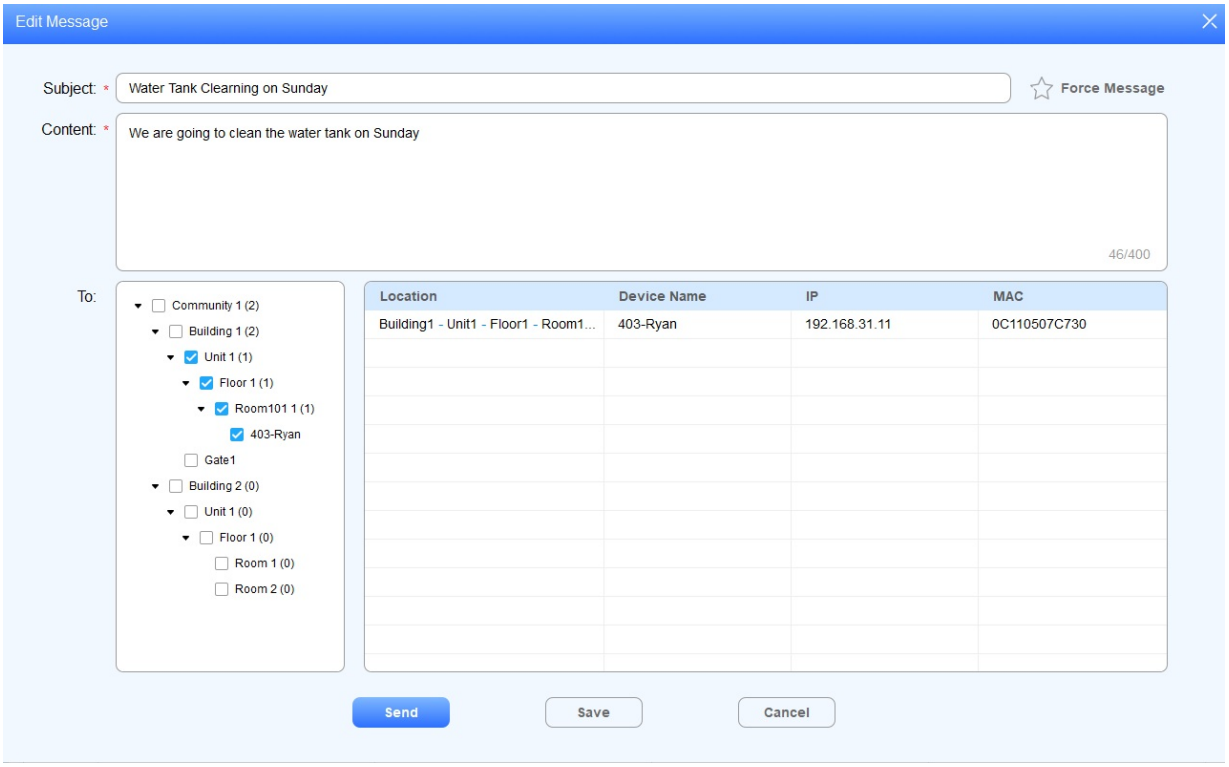
   of the sent message you want to delete , or tick the

   to delete all the sent messages.
2. Click

   of the specific message you want to edit and select the the node two to which you want to send the draft message.



9.3.Ad Pushing

9.3.1.Photo/Video Ads

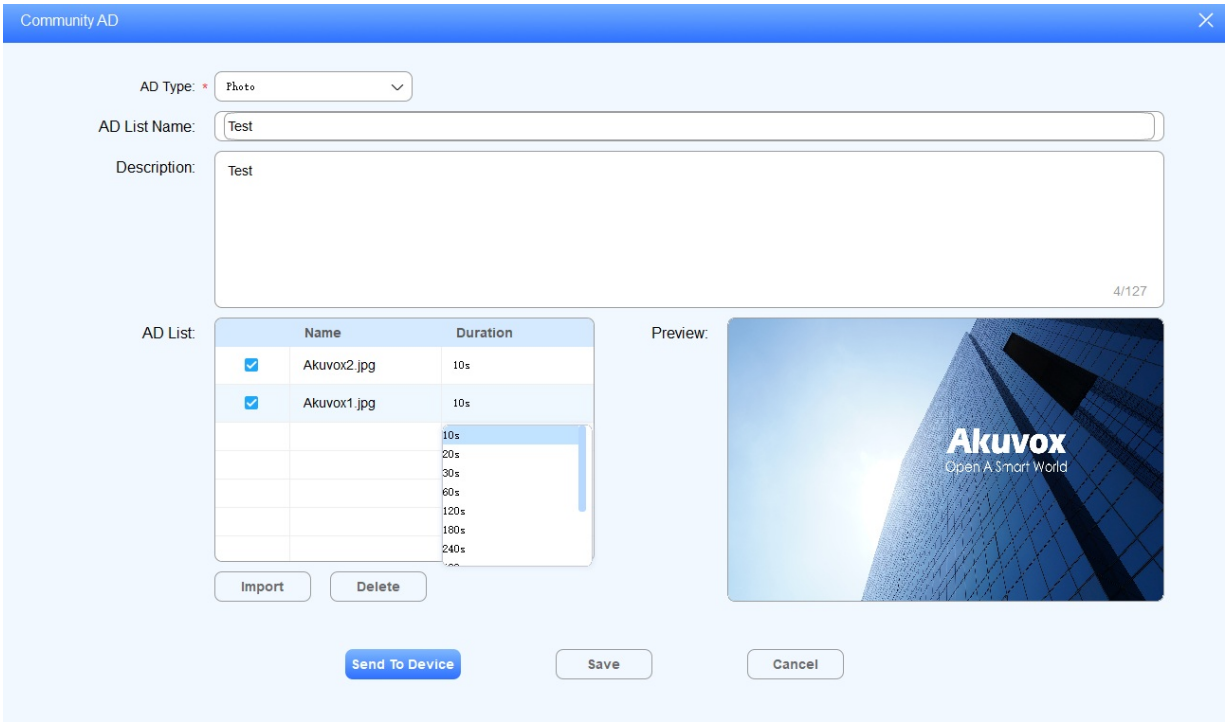
You can upload the Ad pictures videos to the SDMC and synchronize them to the targeted residents' indoor monitor. And the pictures and video will be displayed in rotation according to the display duration you set up.

1. Select **Message > Community ID**.
2. Click
   

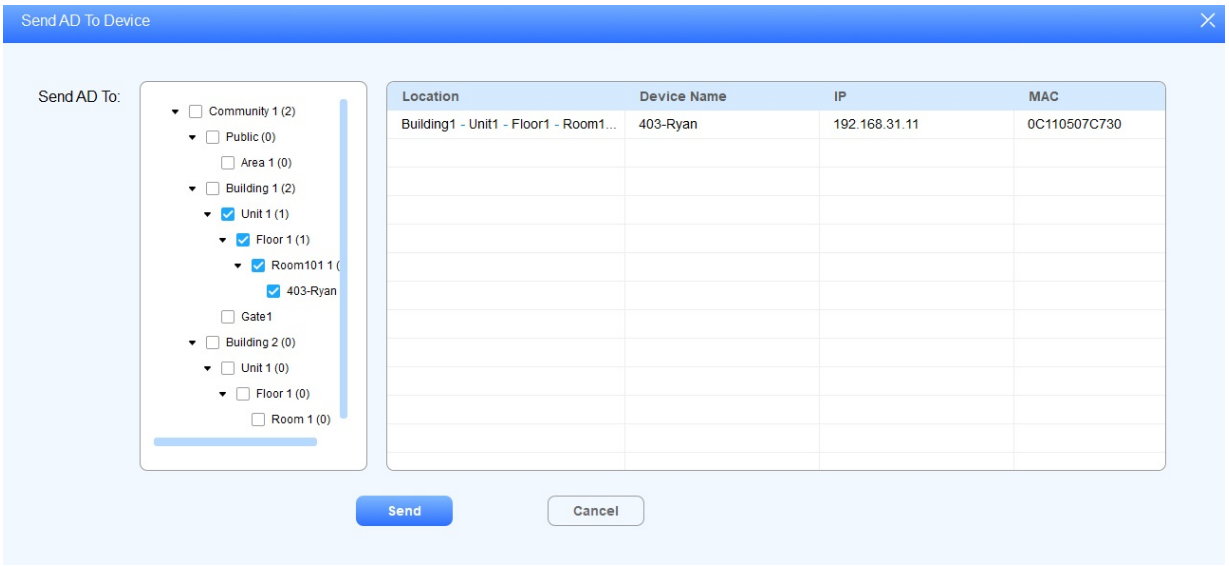
   .
3. Select Ad Type

- **Photo Ad**

1. Create a Ad list name for the picture based on your need.
2. Enter the description for the ad based on your need.
3. Click **Import** to upload the picture to SDMC, and set the display duration.
4. Click **Save** to save the picture, and click **Send To Device** if you want to synchronize the picture to the device.



5.Select the device to which you want to synchronize the picture(s) by nodes, then click Send for the confirmation.



- **Field Name Description:**

NO.	Field Name	Descriptions
1	Ad Type	Select photo or video ad according to you need.

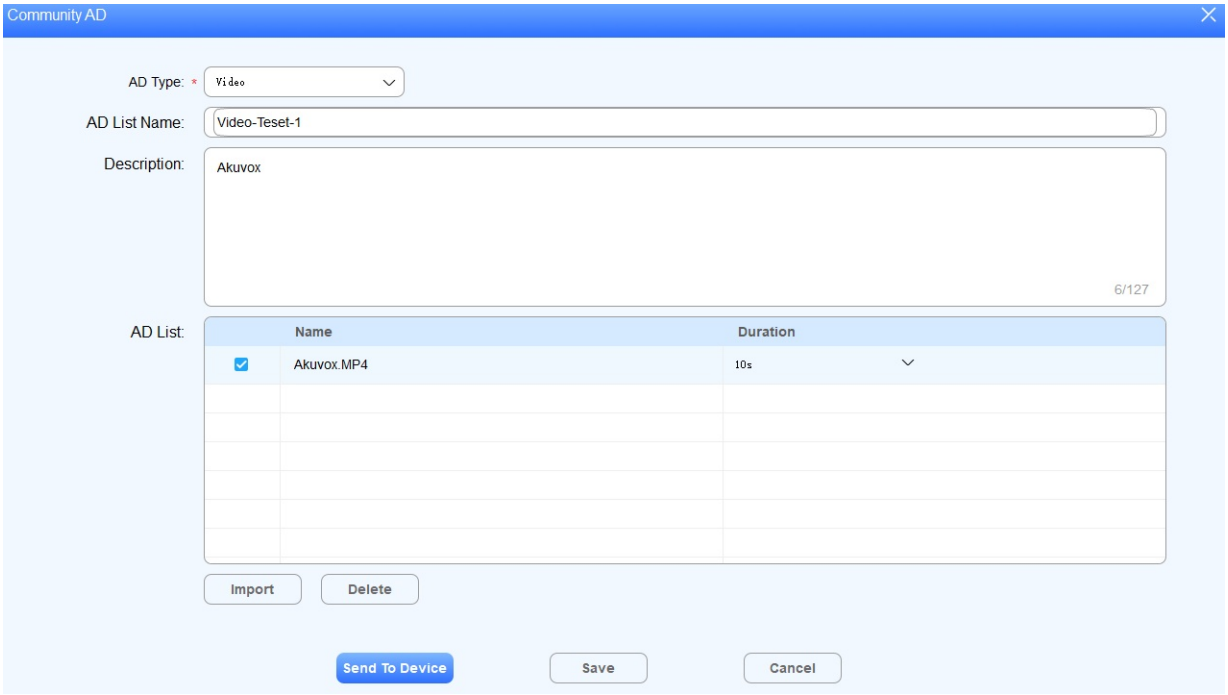
2	AD List Name	Create Ad list name for the convenience of management and categorization
3	Description	Enter the description for ads, for example you can enter the owner of the ads and ad expiration date etc.
4	Name	Shows the file name of the picture
5	Duration	Set the rotational display duration of the pictures. The duration can be 10s, 20s, 30,60s, 120s,180s,240s, 300s, 600s, 1200s, 1800s,3600s, and 10s (default duration). For example, if you select “10s” for the duration, then a picture will be displayed for 10 seconds before it changes to the next one.
6	Preview	Display the preview of the picture.

Note:

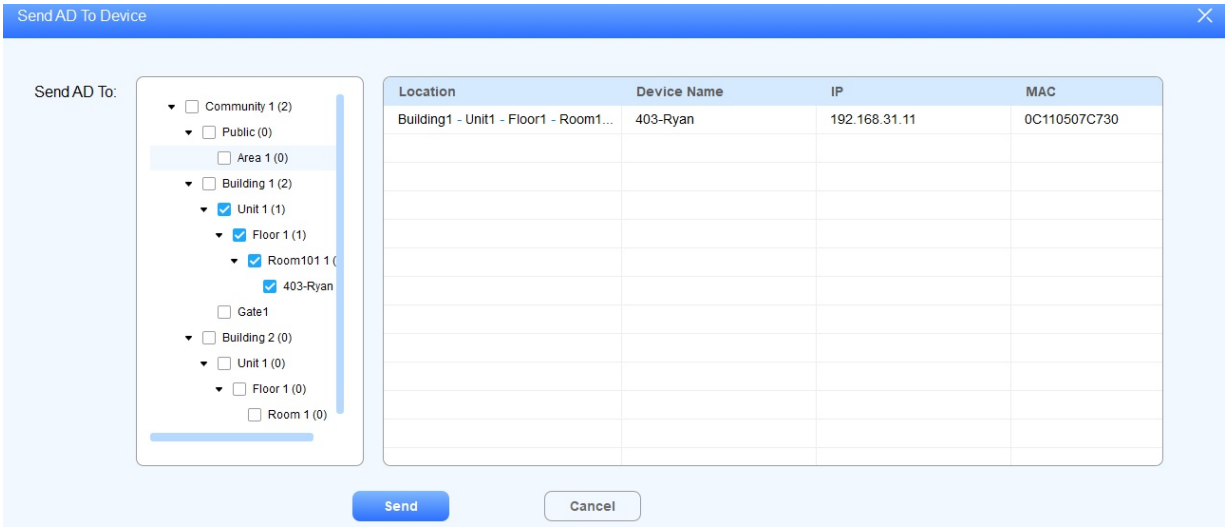
The picture should be .jpg, jpeg, and png format with recommended dimension of 1920*1080 .

- **Video Ad**

1. Create an Ad list name for the video based on your need.
2. Enter the description for the video based on your need.
3. Click **Import** to upload the video to SDMC, and set the display duration.
4. Click **Save** to save the picture, select the video(s) and click **Send To Device** if you want to synchronize the video to the device.



5.Select the device to which you want to synchronize the video(s) by nodes, then click **Send** for the confirmation.



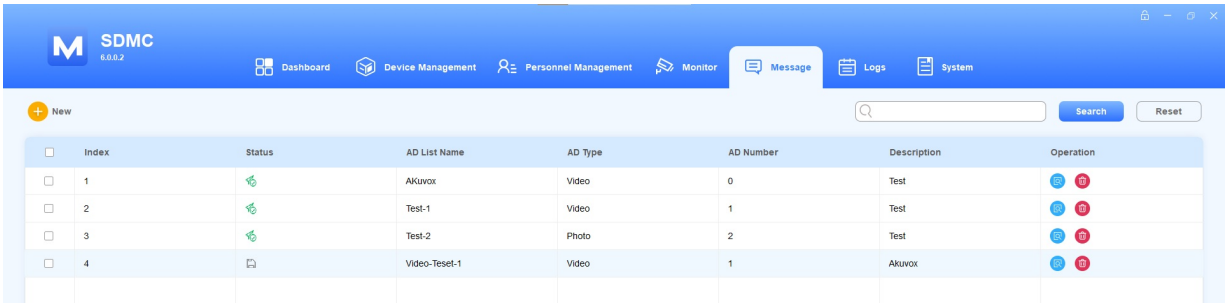
Note:

The video should be mp4, wmv, avi format.

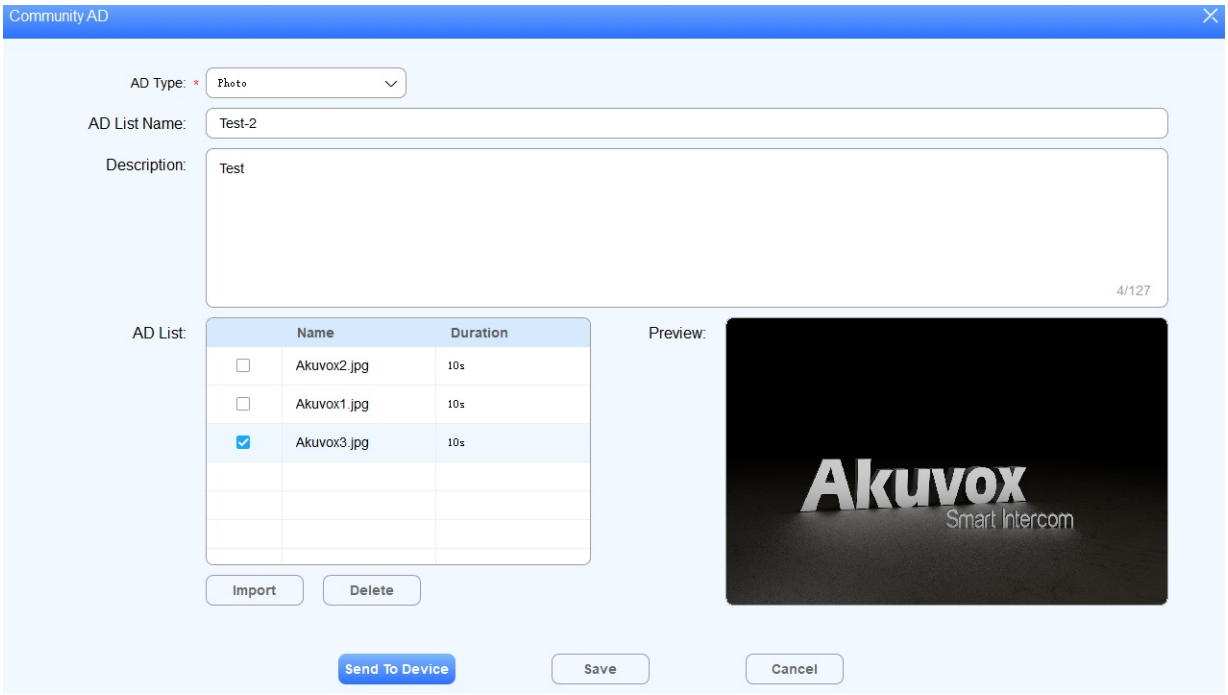
9.3.2.Check/Delete/Edit Ads

1. Select **Message > Community AD**.
2. Search the ads by **Ad List name, Ad Number, and Description** in the fuzzy search field.
3. Click

   of the ad(s) you want to delete, or click **Delete All** if you want to delete all of them.



4.Edit the ads according to your need.



10.Logs

Log module allows you manages four types logs. Namely, **Access Logs**, **Alarm logs**, **Call logs**, **System logs**.

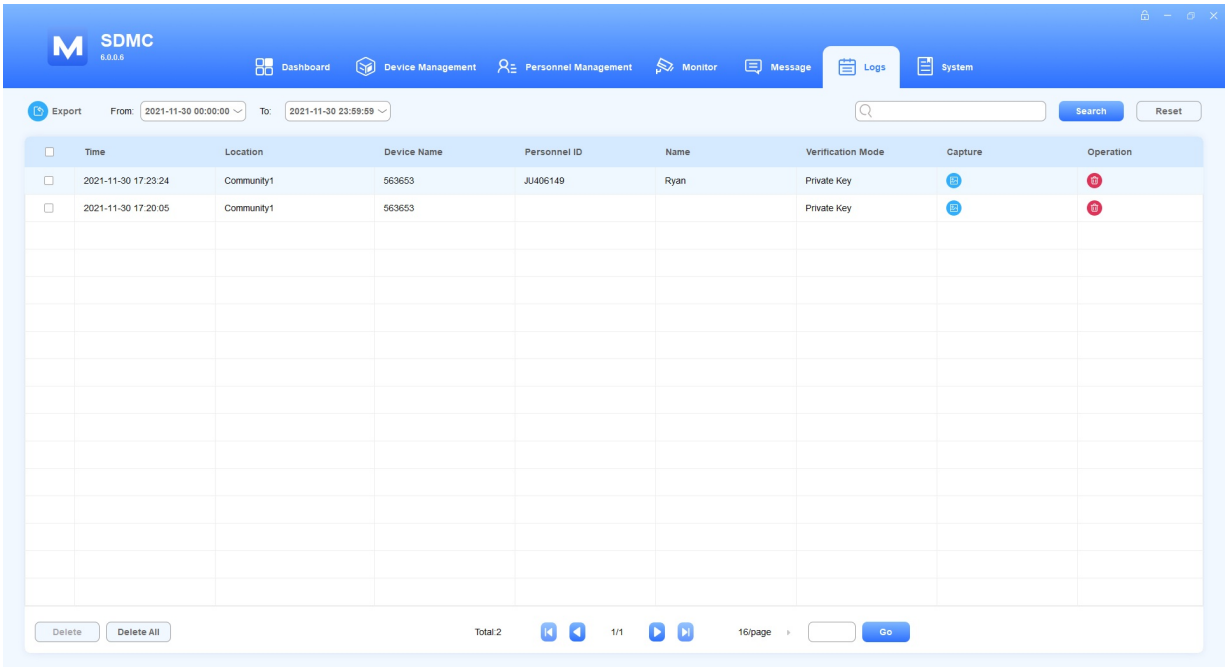
10.1.Access Logs

10.1.1.Search/Check/Delete Access Logs

1. Click **Logs** Module, and select **Access Logs**.
2. Search the access log by **Name**, **Location**, **Personnel ID**, **Device Name**, in the search field
3. Click

   to see the picture captured.
4. Click

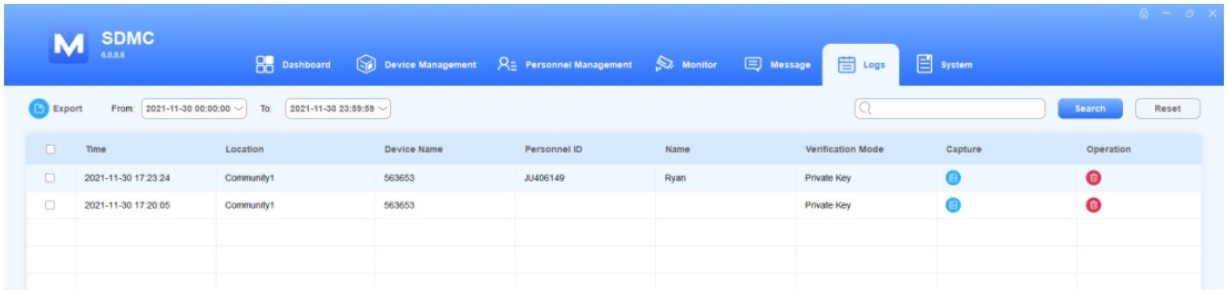
   of the log you want to delete, or click **Delete All** if you want to delete all the logs.



10.1.2. Export Access Logs

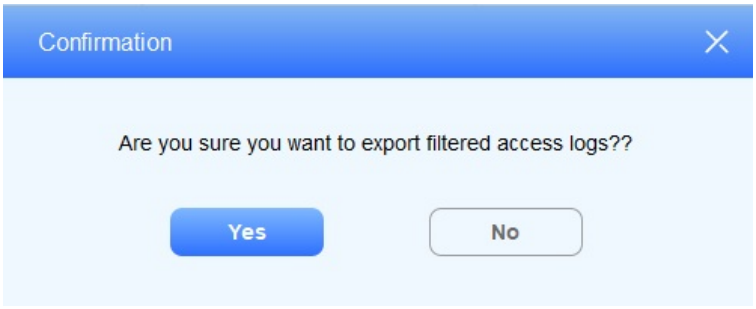
You can export Access Logs if needed.

1. Click **Logs** Module, and select **Access Logs**.



2.Click

to export the log to your PC.



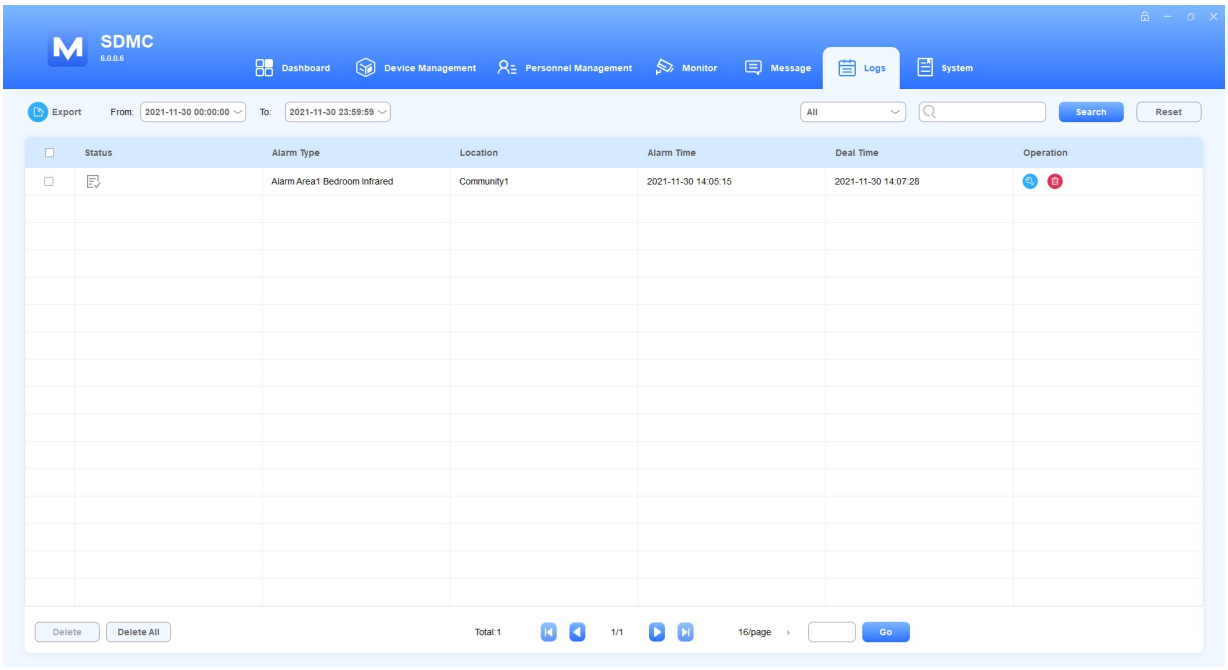
10.2. Alarm Logs

10.2.1. Search/Check/Delete Alarm Logs

1. Click **Logs** Module, and select **Alarm Logs**.
2. Search the alarm log by **All/Dealt/Undealt/**, **Location**, in the search field.
3. Click

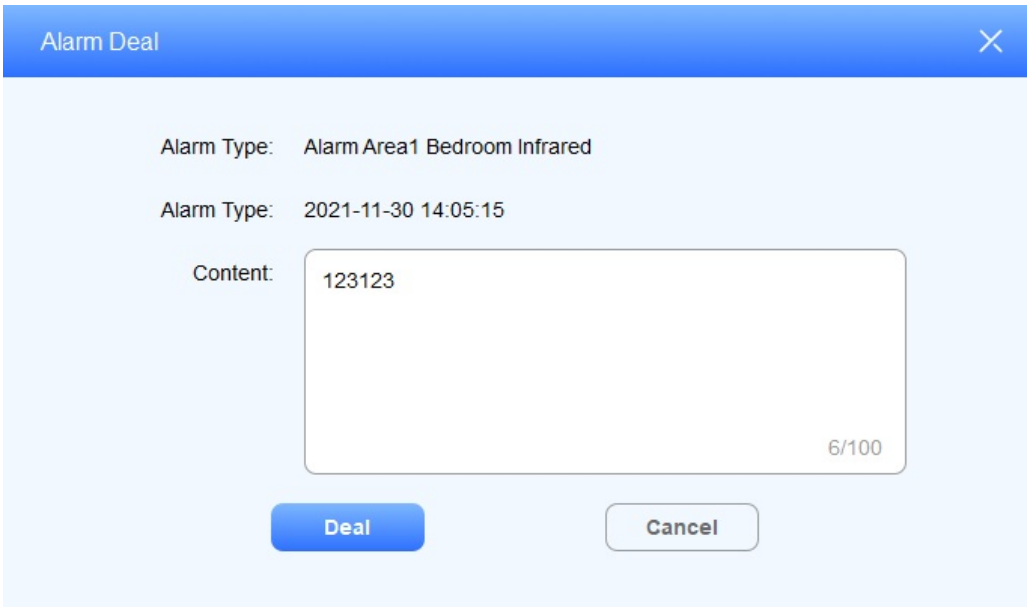
   to see the picture captured.
4. Click

   of the log you want to delete, or click **Delete All** if you want to delete all the logs.



5.Click

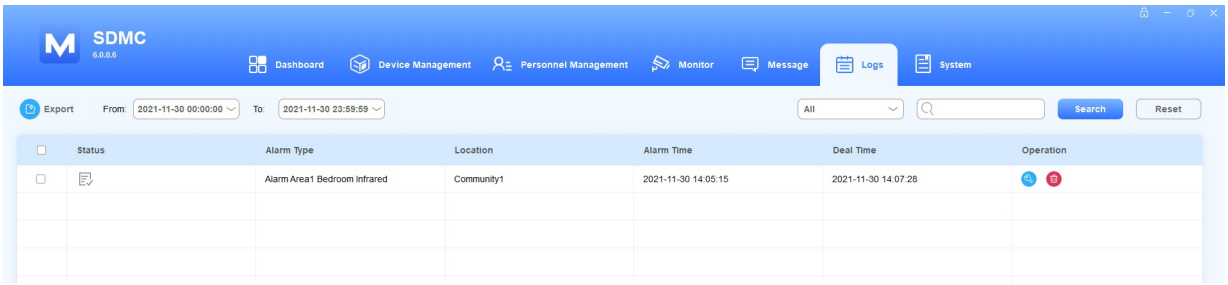
of the alarm logs if you want to enter remarks for the alarm you have dealt.



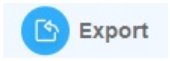
10.2.2. Export Alarm Logs

You can export Alarm Logs if needed.

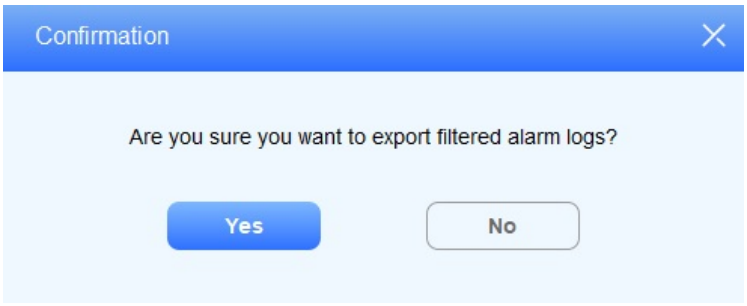
1. Click **Logs** Module, and select **Alarm Logs**.



2.Click



to export the log to your PC.

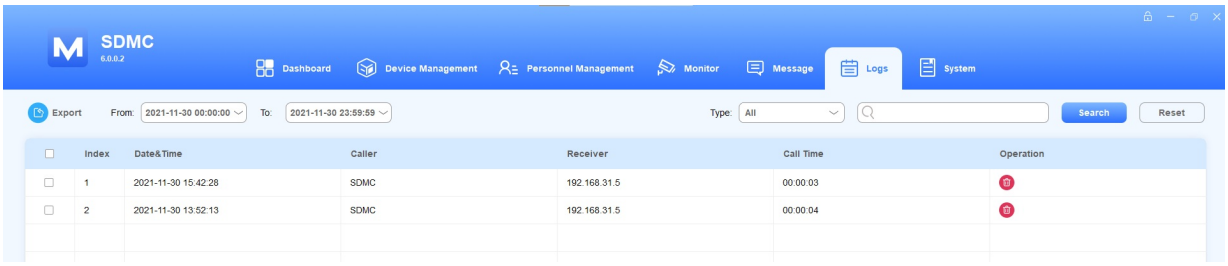


10.3. Call logs

10.3.1. Search/Check/Delete Call Logs

1. Click **Logs** Module, and select **Call Logs**.
2. Search the call log by date, by type, and location in the search field.
3. Click

   of the log you want to delete, or click **Delete All** if you want to delete all the logs.

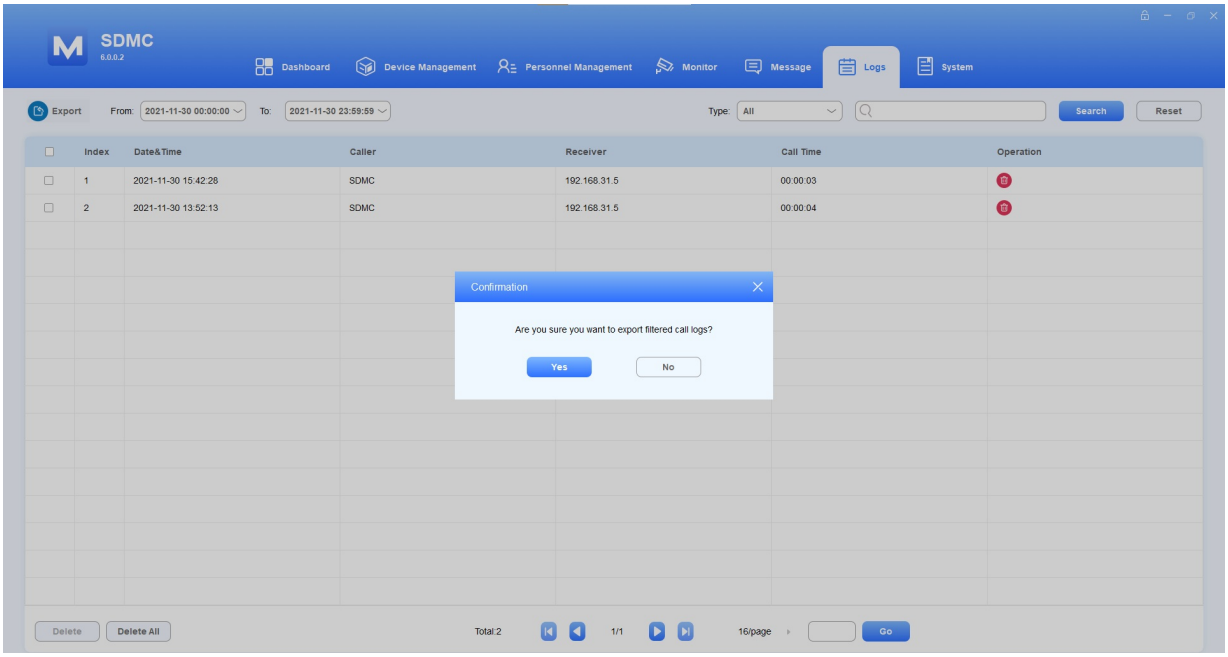


10.3.2. Export Call Logs

You can export Alarm Logs if needed.

1. Click **Logs** Module, and select **Call Logs**.
2. Click

   to export the log to your PC.



10.4. System Logs

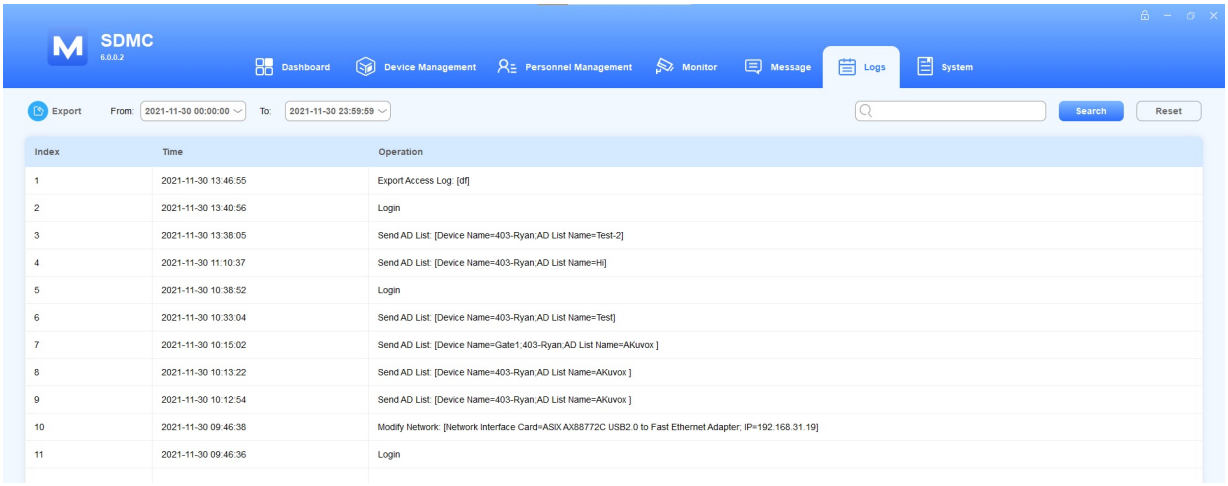
System module allows you to monitor all the system operations that have occurred in the SDMC. You can check system logs and export the log to your PC if needed.

10.4.1. Search/Export Logs

1. Click **Logs** Module, and select **System Log**.
2. Search the logs by date and by keyword in the search field.
3. Click

   to export the system logs to your PC.



- **Operation code examples**

System log is composed of the operation code starting with a verb .

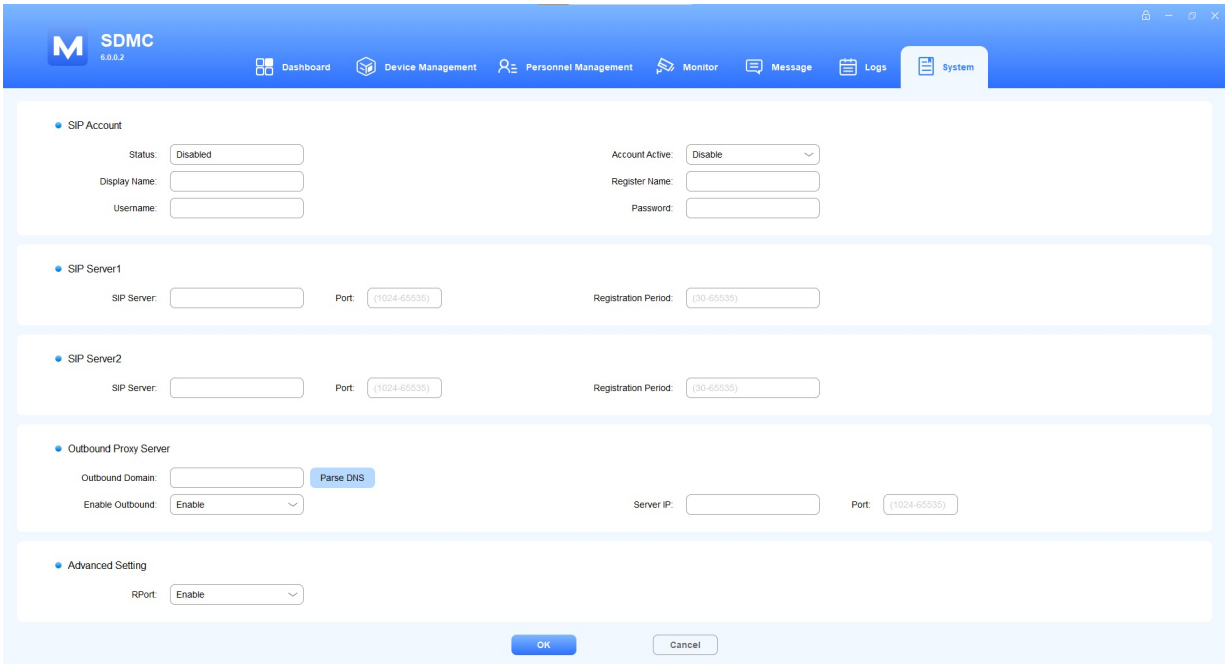
NO.	Operation Verb	Descriptions
1	Login	Indicates an Login operation meaning some one has log in to the SDMC
2	Send	Indicates an **Send** operation, for example" Send AD List: [Device Name=403-Ryan; Adlist Name=Test-2" means AD list has been sent to the device (403-Ryan) with Ad list name " Test-2"
3	Modify	Indicates an **Modfiy** operation,Modify Network [Network Interface Card=192.168.31.15, IP=192.168.31.19, meaning the network adaptor IP address has been changed to 192.168.31.19

11.System

11.1.SIP Setting

You are required to configure SIP setting for the SDMC before you can make SIP calls from SMDC to the devices.

1. Click **System** Module, and select **SIP Setting**.
2. Configure the SDMC SIP setting.



- **Field Name Description**

NO.	Field Name	Descriptions
SIP account	Status	Displays if the SIP account is registered or not. It will show “**Enabled**” if the account is not registered.
Account Active	Enable or disable the registered SIP account	
Display Name	Configure the name, for example the device’s name to be shown on the called-party device. You can fill in 63 bytes of characters in length maximum.	
Register Name	Enter the SIP account register Name obtained from the SIP account administrator. You can fill in 63 bytes of characters in length maximum.	
Username	Enter the SIP account register Name obtained from the SIP account administrator for authentication. You can fill in 63 bytes of characters in length maximum.	
Password	Enter the password obtained from the SIP account administrator for authentication.	
SIP Server1/2	SIP server	Enter the SIP server IP address or its URL.
Port	Set SIP server port for data transmission	
Registration	Set SIP account registration time pan. SIP re-registration will start automatically if the account registration fails during the registration time span. The default registration period is “**1800**”, ranging from **30-65535**s.	

Outbound Proxy Server	Outbound Domain	Enter the domain name (DNS) provided by the outbound proxy server provider.
Enable Outbound	Enable the outbound proxy server.	
Server IP	Enter the Outbound SIP server IP address or its UR	
Port	Enter the outbound SIP server port for data transmission	
Advanced Setting	RPort	Enable the Rport when the SIP server is in WAN (**Wide Area Network**).

Note:

An outbound proxy server is used to receive all initiating request messages and route them to the designated SIP server for the data transmission.

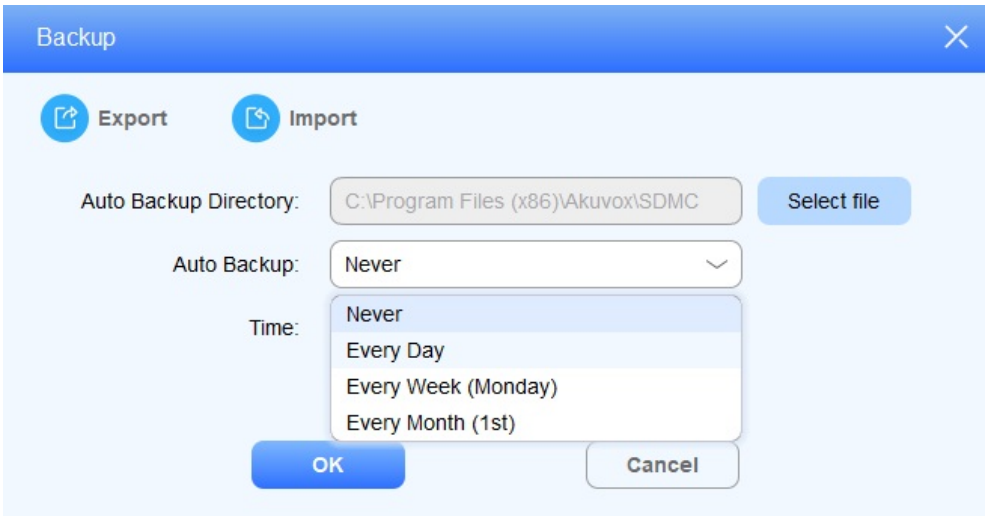
11.1.1. Import/Export/backup Database

You can export the SDMC data to your local PC as a backup, which can be used to restore your SDMC database when n data damage or data breakdown occurs. You can set the auto backup schedule for the database.

1. Click **System** Module, and select **Database**.
2. Set the auto backup schedule for the SMDC database if need. Database is used to restore the database when data damage or data breakdown occurs.
3. Click 

to upload the .db file (database) from your local PC to SDMC.
4. Click 

to export the .db file (database) to your local PC.



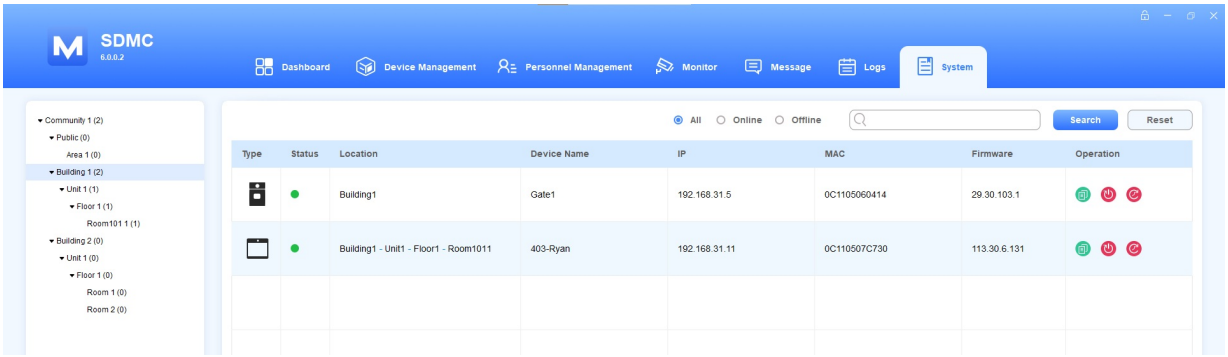
11.2.Device Autop Data Backup

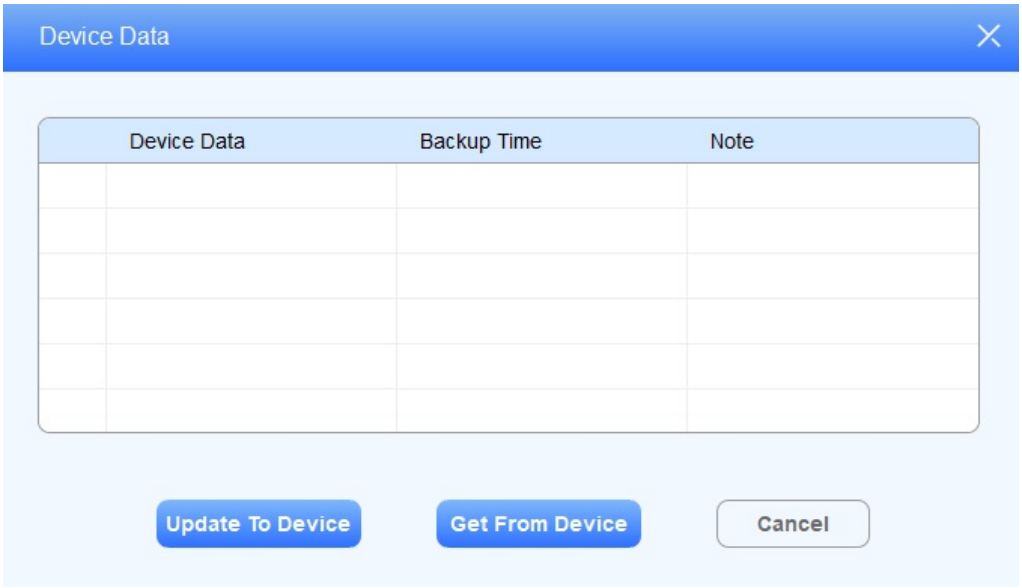
11.2.1.Update Autop Data to Device

1. Click **System** Module, and select **Device Data Backup**.
2. Select the the device by node on the left column or search the device by **Device Name**, **MAC etc.**
3. Click

   of the device to which you want to update the AutoP data.

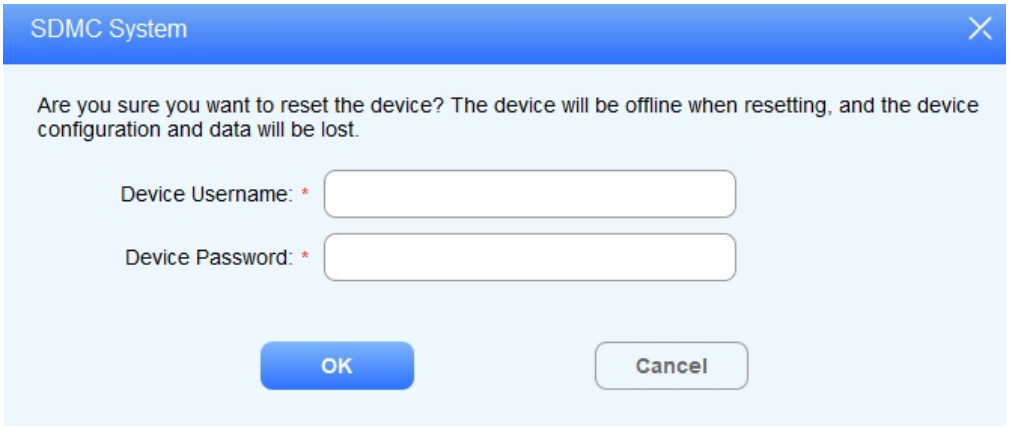




11.2.2. Reset the device

You can reset the device remotely from your SDMC for the device maintenance and troubleshooting etc.if needed.

1. Click **System** Module, and select **Device Data Backup**.
2. Select the the device by node on the left column or search the device by **Device Name**, **MAC etc**.
3. Click  of the device you want to reset.
4. Enter the authentication username and password.



11.2.3. Reboot the device

You can reboot the device remotely from your SDMC for the device the maintenance and troubleshooting etc.if needed.

1. Click **System** Module, and select **Device Data Backup**.
2. Select the device by node on the left column or search the device by **Device Name**, **MAC etc**.
3. Click  of the device you want to reboot.
4. Enter the authentication username and password.

11.3. Lift Control

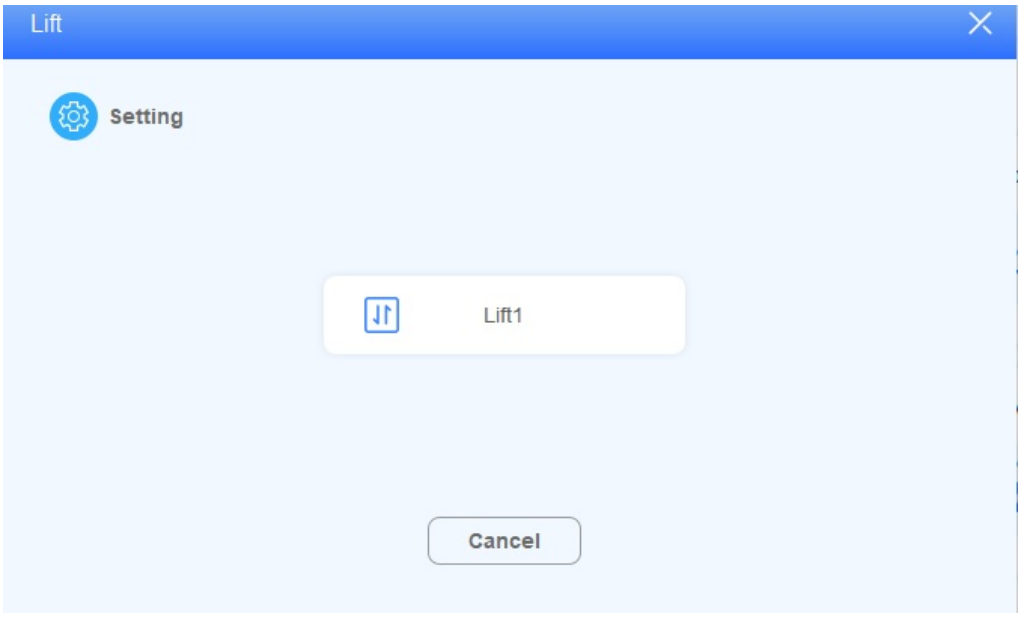
1. Click **System** Module, and select **Lift Control**.
2. Click on

of the lift you want to control.

1. Enable the lift, and edit the lift label.
2. Enter the lift-control HTTP command provided by the life controller manufacturer. Then back out.

Click

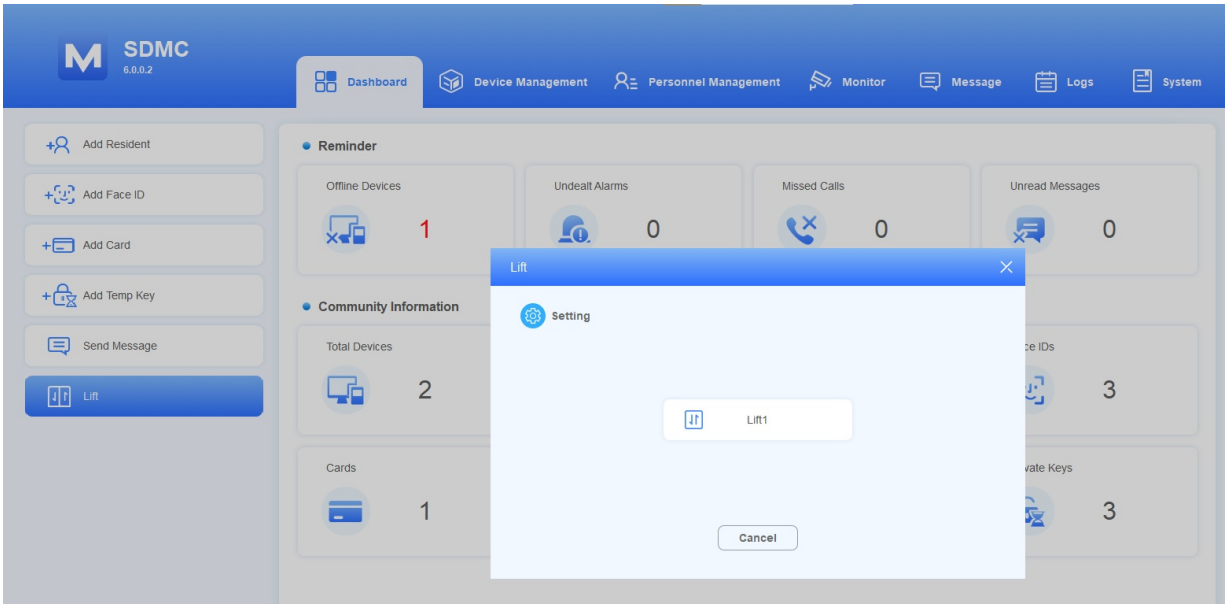
on Lift to summon the lift.



- Field Name Description:

NO.	Field Name	Descriptions
1	Enable	Enable it so that you can configure the lift control
2	Label	Configure the lift label 1-6. The label should be 63 digits maximum in length.
3	HTTP command	Enter the HTTP command, which should be 255 digits maximum in length.

Lift control can also be made on the dashboard.



11.4. System Setting

11.4.1. Quick Entrance

Quick Entrance allows you to configure operational icons on the dashboard for the quick and convenient of operations.

1. Click **System** Module, and select **System Setting**.
2. Click Quick Entrance.
3. Move the operational icons left or right using

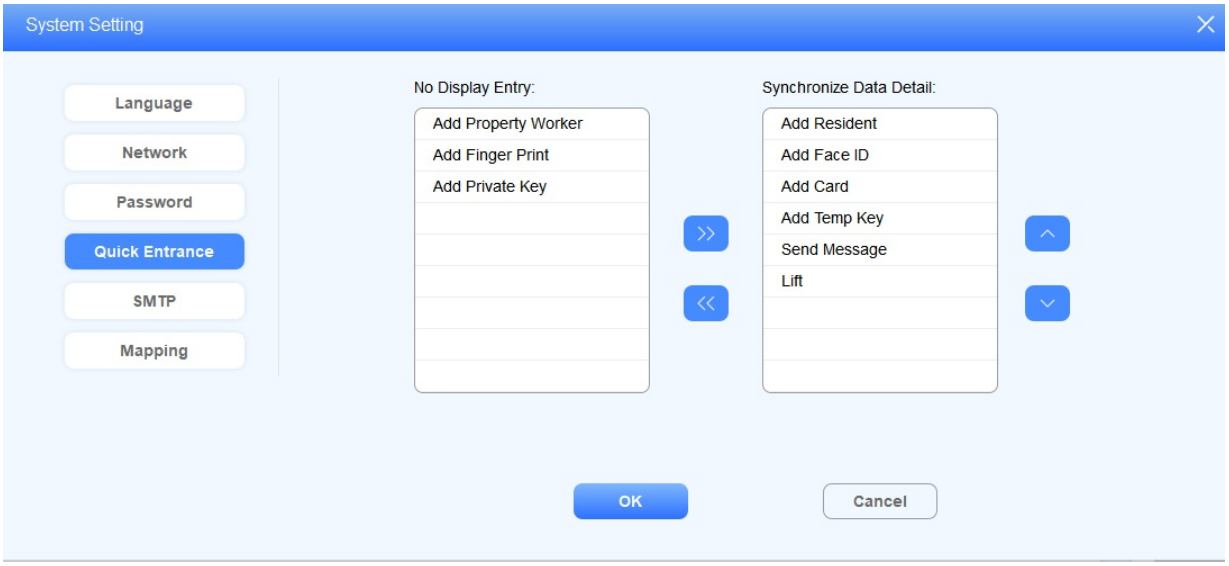
   

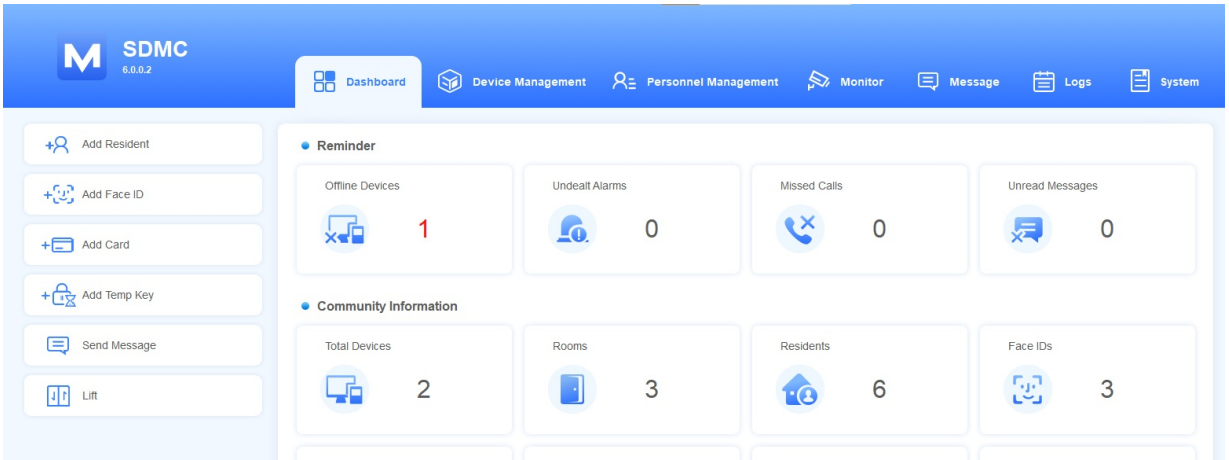
   and adjust the dashboard position of the operational icons selected using

   according to your need.

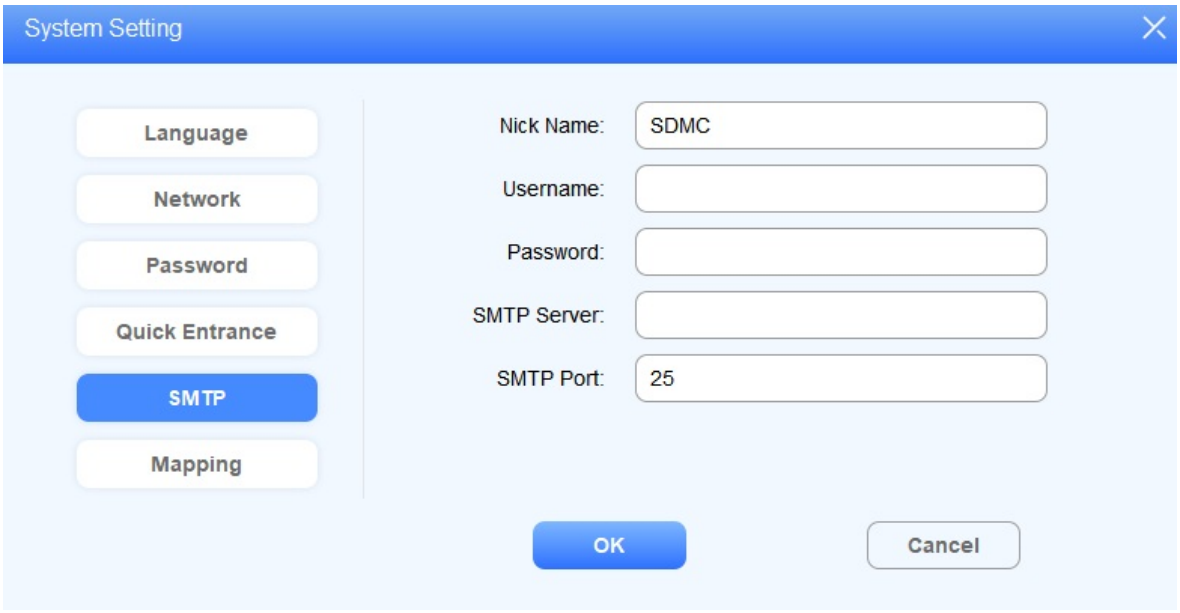




11.4.2. SMTP

SMTP server can be configured in your SDMC. When alarm goes off or door is unlocked, then notification can be sent to the SMTP server.

1. Click **System** Module, and select **System Setting**.
2. Click **SMTP**.



- **Field Name Description:**

NO.	Field Name	Descriptions
1	Nick Name	Enter the sender name of the notification, which is SDMC by default. The sender name should be 63 digit maximum in length.
2	Username	Enter the SMTP server authentication username.
3	Password	Enter the SMTP server authentication password
4	SMTP Server	Enter the SMTP server address. It should 255 digit maximum in length
5	SMTP Port	Enter the SMTP server port ranging from 1-65535. 25 is the initial default number.

12.Contact Us

For more information about the product, please visit us at www.akuvox.com or feel free to contact us by

Sales email: sales@akuvox.com

Technical support email: support@akuvox.com

Telephone: +86-592-2133061 ext.7694/8162

We highly appreciate your feedback about our products.

↑