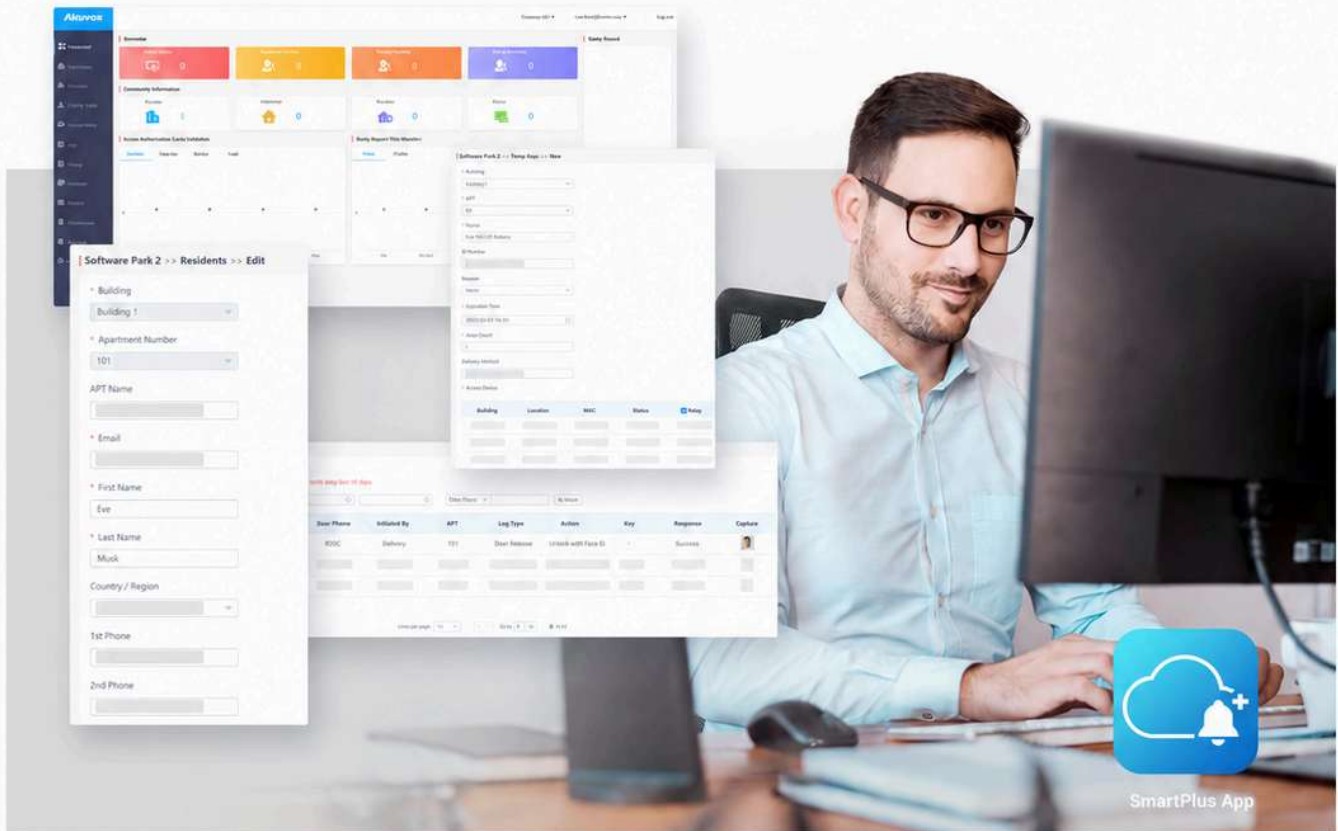


Akuvox V7.4.1 Smart Access Single-Company Project Management Guide

UPDATED

Updated on Jun 8, 2026 • Published on Nov 20, 2025





AKUVOX SMART ACCESS USER GUIDE

Project Manager



Update Time: May. 2026

This manual is intended for both installers and project managers(PMs) who need to manage single-company commercial projects, including personnel and devices on the Akuvox Smart Access Cloud (**Version: 7.4.1**).

For more information, please visit <http://www.akuvox.com/> or consult Akuvox technical support.

Note

- The project created before **October 15, 2024** remains the old settings. To learn about the setup, project managers can refer to [Akuvox V6.8.1 SmartPlus Property Manager Guide - Office](#).
- For installers, this manual contains the feature setup in specific projects. To learn about installer portal's features including site management, sub-account management, and subscriptions, please refer to [Akuvox Smart Access Installer Portal Guide — Commercial Projects](#).

What's new in version 7.4.1:

- [Support assigning a personnel to multiple groups when editing the personnel import template.](#)
- [Support batch editing personnel using a template.](#)
- [Adjust the Multiple In/Out times from 8 to 15 in the Attendance feature.](#)

System Overview

You can use this platform to:

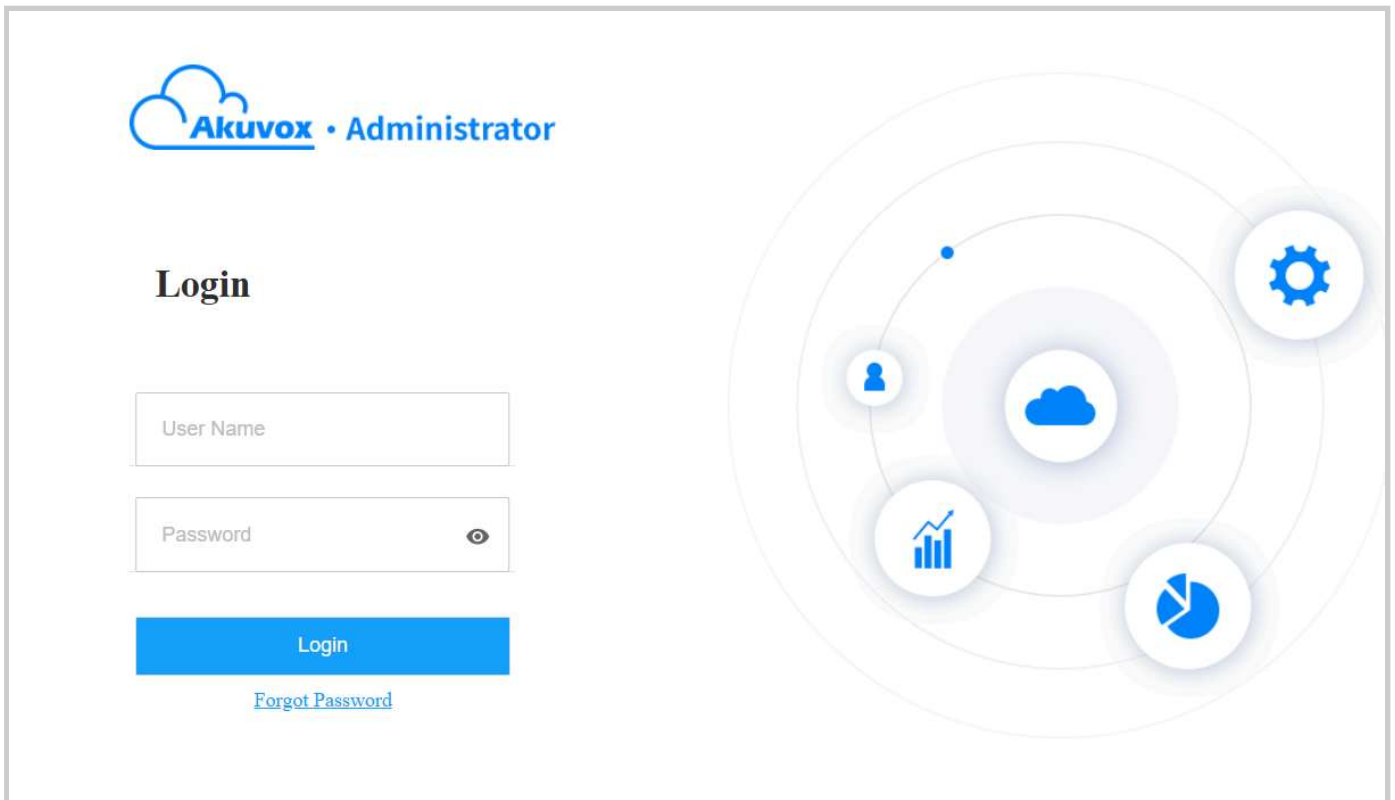
- Add, edit, and delete administrators, personnel accounts, devices, etc.
- Deploy and set up devices and doors for access control.
- Set up access groups and holiday schedules.
- Set up access methods for visitors.
- Set up attendance and smart parking.
- Check various logs such as door logs, call history, and alarm records.



Login

Log in to the smart access platform with your account. For installers, the account is created by your distributor; for project managers, the account is created by your installer.

1. Open the web browser, enter the address (URL) of the cloud server location in your area, and click **Enter**.
2. Enter your username and password.
3. Click **Login**.



The screenshot shows the login interface for the Akuvox Administrator. At the top left is the logo, which consists of a blue cloud icon followed by the text "Akuvox • Administrator". Below the logo, the word "Login" is displayed in a bold, black font. Underneath "Login" are two input fields: the first is labeled "User Name" and the second is labeled "Password" with a small eye icon to its right. Below these fields is a blue button with the text "Login" in white. Under the button is a link that says "Forgot Password". To the right of the login form is a large, light blue circular graphic. This graphic features a central cloud icon surrounded by four smaller circular icons: a person icon, a bar chart icon, a pie chart icon, and a gear icon. These icons are connected by a circular line, suggesting a system or network architecture.

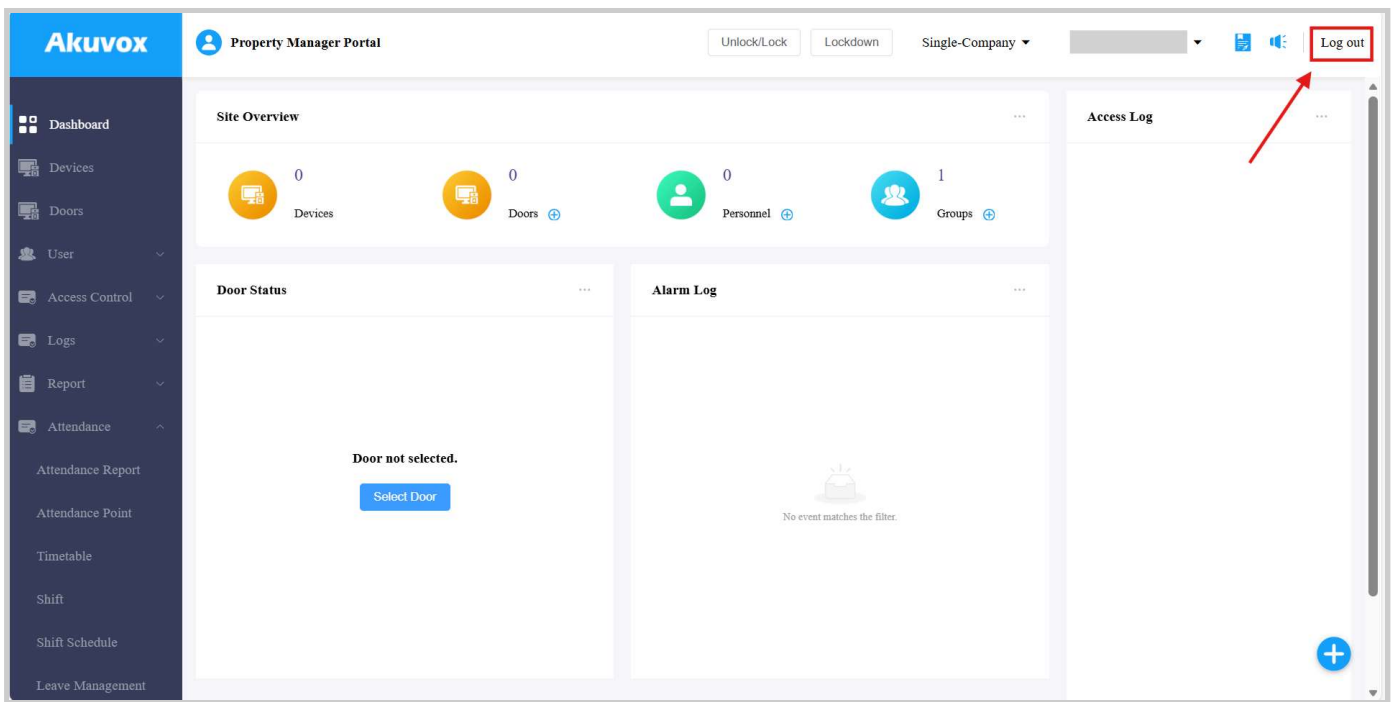
Note

Enter the verification code sent to your email address for login when your distributors or installers enable the Two-factor Authentication feature.

Log Out

Click on **Log out** in the upper-right corner to exit the system.





Prior to the Management

It is advised that you go through what is listed below before starting management.

- Check if all device MAC addresses have already been registered by your distributor.
- Check if the device firmware supports cloud mode with no connection to SDMC.
- Check if the device is powered on and is connected to the internet, and make sure that the network is normal.
- Check and make sure that the user information and device information are correct.

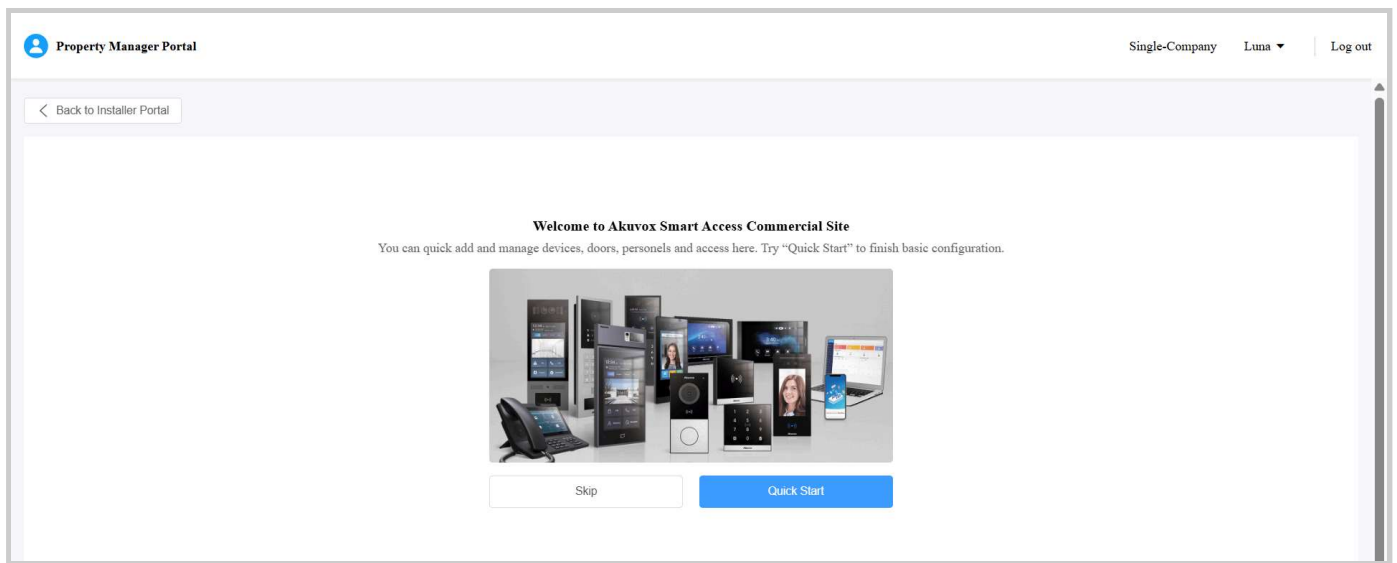
Quick Start

The first time you manage the project, quickly set it up through the quick start instructions.



Or, skip to set it up later.

- As an installer, you can set up devices, personnel, and access groups.
- As a project manager, you can set up personnel and access groups.



Note

Click [here](#) to view the detailed configuration steps in the quick start.

Dashboard

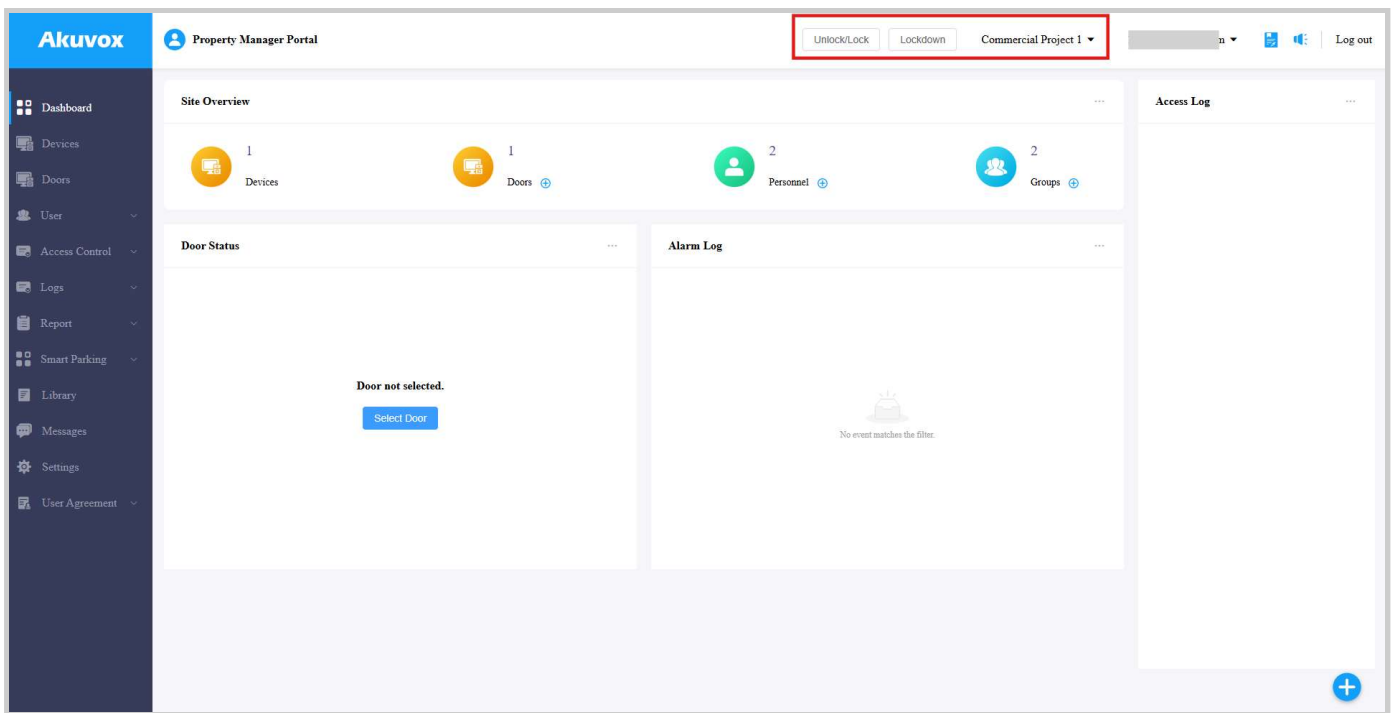
The project management dashboard gives you an overview of the commercial project.

As the permissions of PMs and installers are different, the dashboard also differs slightly.

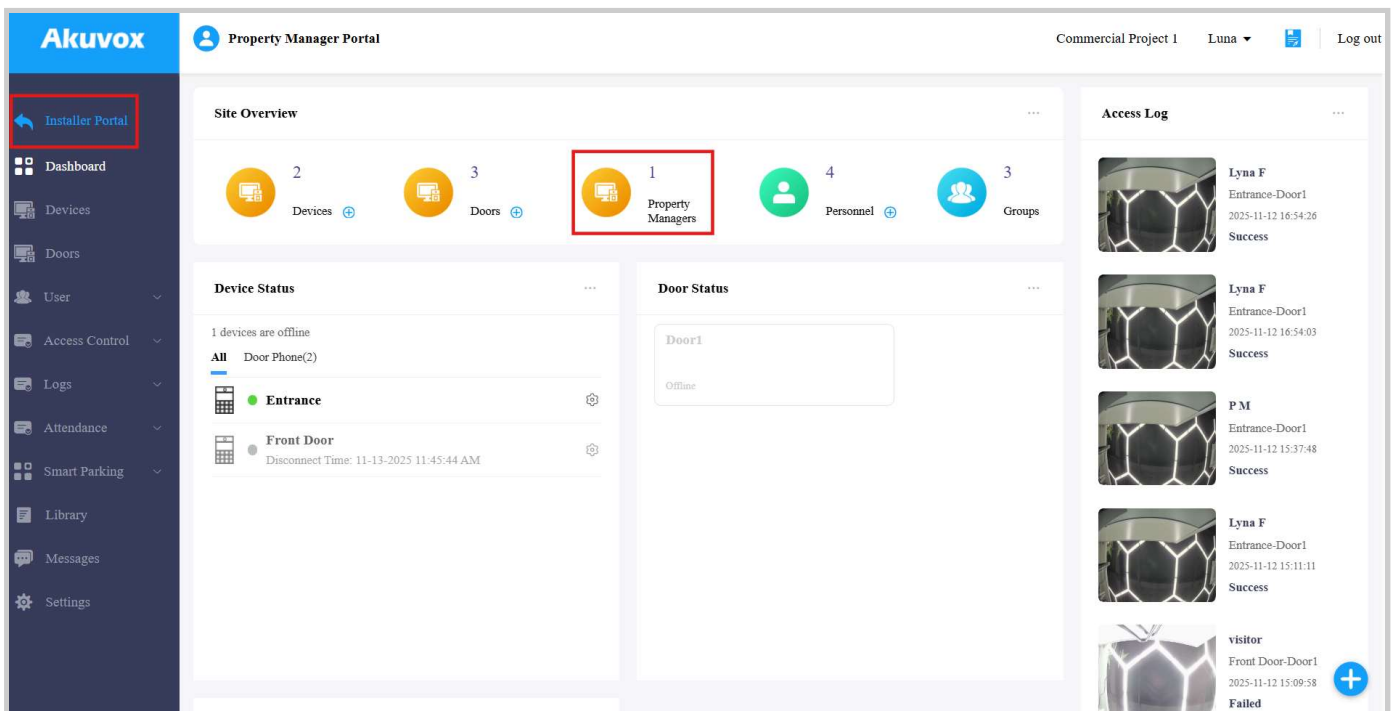
- Installers can add devices, check device status, check PM number, and return to the installer web portal on the dashboard, but CANNOT perform emergency action(Unlock/Lock) and lockdown, and set up muster report.
- PMs can switch between different projects by clicking the project name in the top menu.

For Project Managers:





For Installers:



Left Menu Description:

Modules	Description
Dashboard	Have a quick grasp of the project management portal.
Devices	Manage devices.
Doors	Manage doors.



Users	Manage personnel, visitors, and administrators.
Access Control	The module contains: • Access Group: Define the schedule that limits entry and exit. • Holiday: Define the holidays that limit entry and exit. • Area Restrictions: Set the anti-passback rules for access.
Logs	Check various logs, including door logs, call history, capture, and alarm records.
Report	Set up and manage muster reports and event reports. Muster reports are ONLY available for project managers.
Attendance	Set up attendance points, check attendance reports, manage, etc.
Smart Parking	Register license plates and UHF tags for users, and manage lots.
Library	The storage of PIN codes and RF cards for quick and integrity management.
Messages	Create and send messages to specific personnel and devices.
Settings	This module includes: • Basic Setting: project name, address, etc. • Time Setting: time zone, time format, and date format. • Motion Setting: motion detection type and alert delay time. • Emergency Setting: emergency door group and emergency permission.

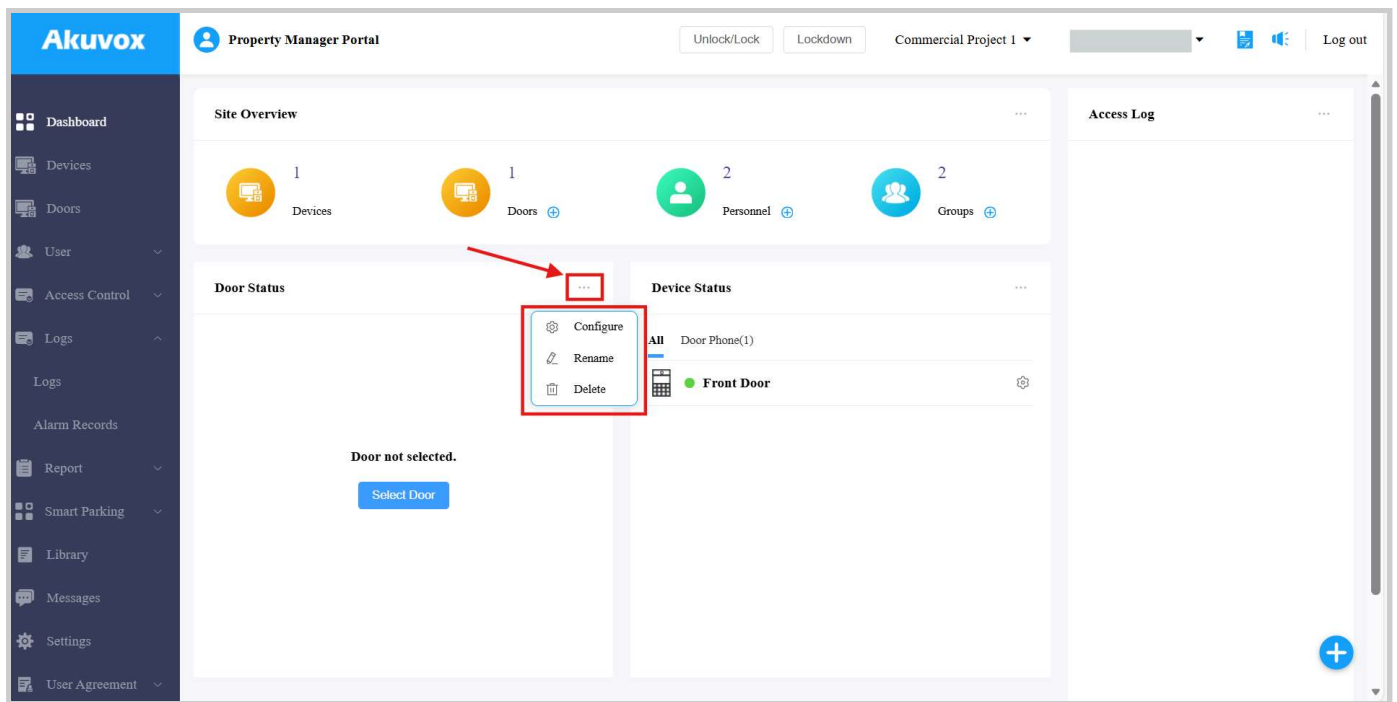
Customize Dashboard

You can customize the dashboard by adding and editing components to match your preferences.

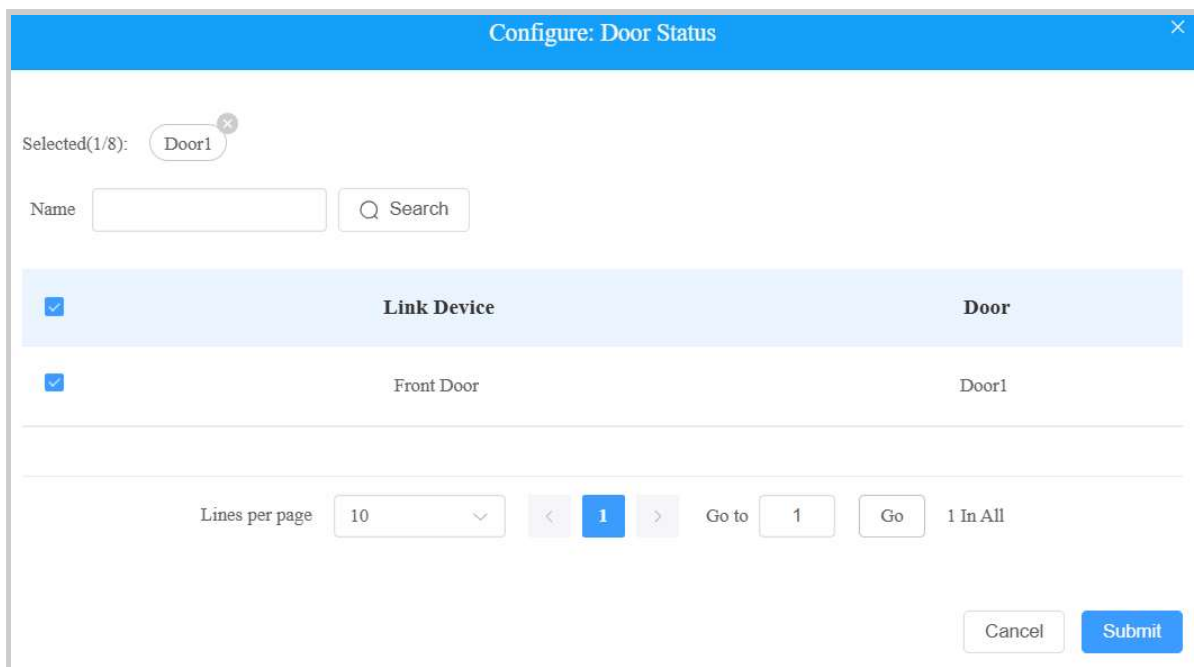


Edit and Remove Components

1. Click  in the upper-right of a specific component.
2. Rename, delete, or configure it.



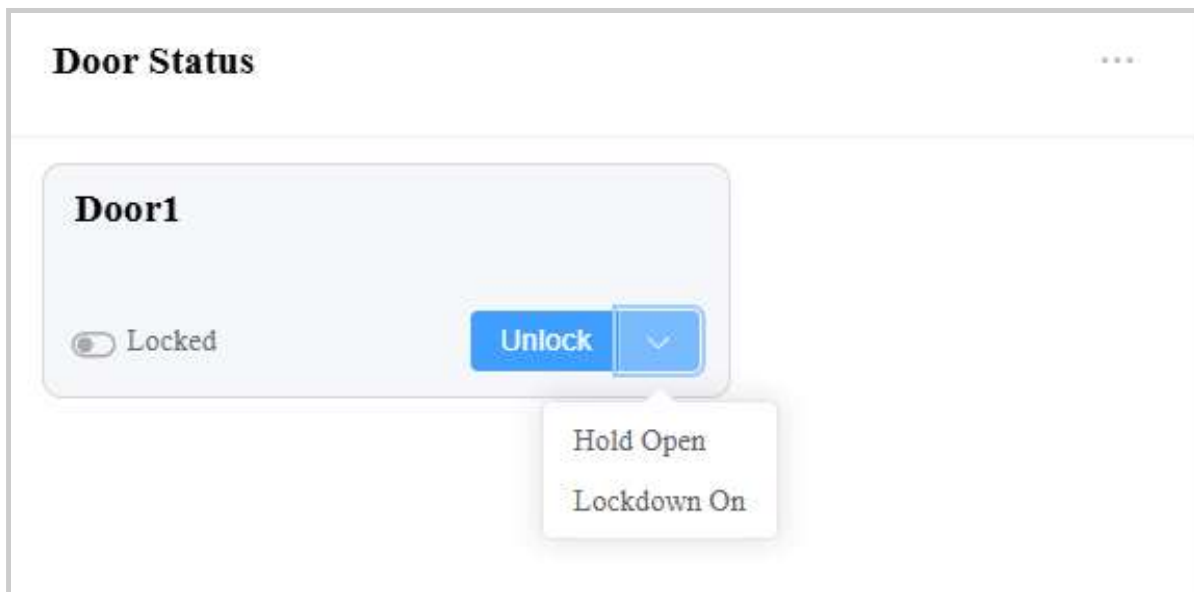
For the **Door Status** component, you can select up to 8 doors to display.



After displaying the door, you can unlock it, lock it down, and hold it open.

ONLY PMs can open/close the door; installers cannot.





Note

- If the system fails to obtain the status of the door, check whether the real-time monitoring feature is enabled on the device side. Click [here](#) to view the configuration steps.
- Specific models and versions support opening/closing doors. See the [Door Management](#) chapter.

For the **Alarm Log** component, you can select the log type to display and set the time of logs.



Configure: Alarm Log

* Alarm

Emergency Alarm × Arming Alarm × ^

Time Interval

All Alarms

Emergency Alarm ✓

Arming Alarm ✓

Door Opened Timeout

Tamper Alarm

Break-in Alarm

For the **Device Status** component, you can select up to 20 devices to display.

Configure: Device Status

* Devices

All Devices × v

Filter

☒ Online

☒ Offline

Cancel

Submit

After displaying the device, click  to redirect to the device's settings interface.

The green dot indicates the device is online.



Device Status

...

All

Door Phone(1)



Front Door



For **Elevator Control** component, click the elevator control device to unlock, hold open, and restore selected floors.

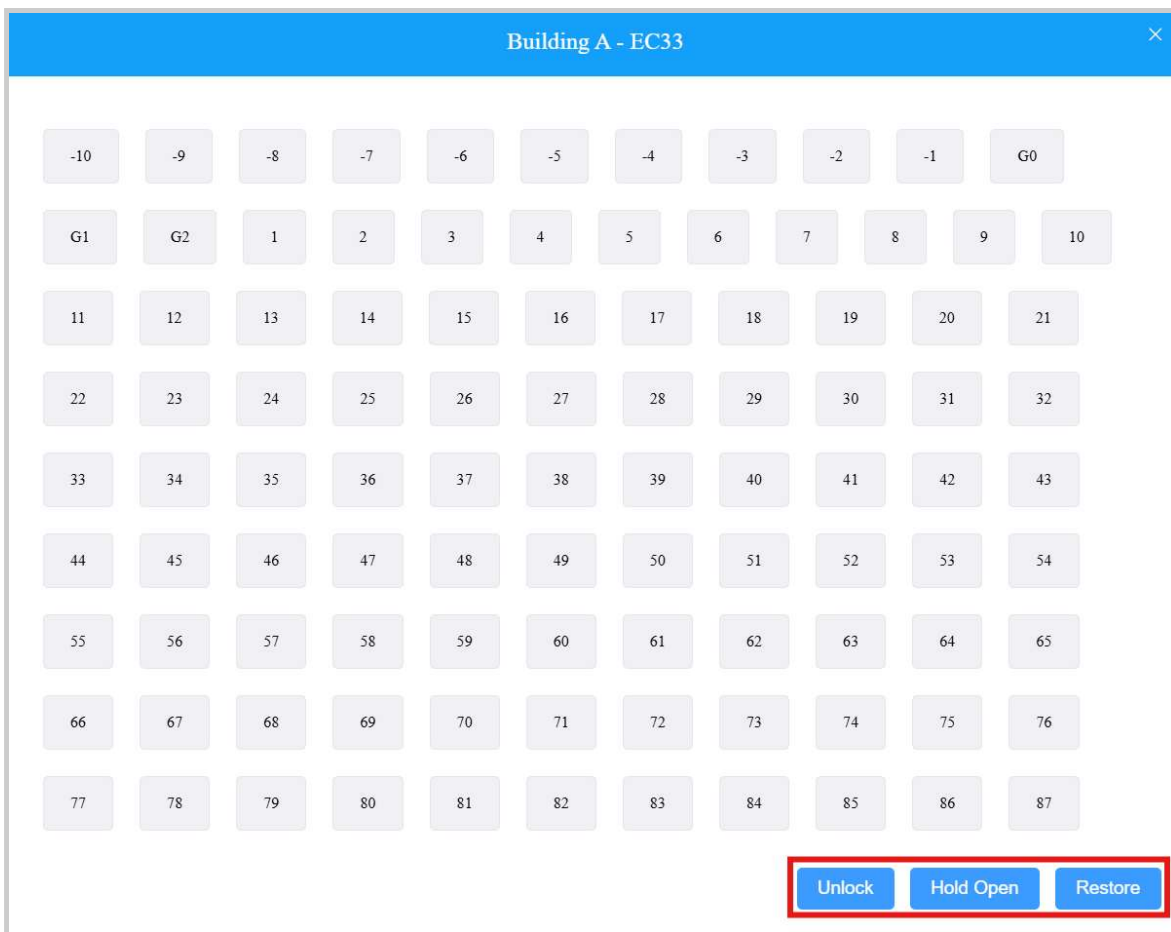
Elevator Control

...

EC33

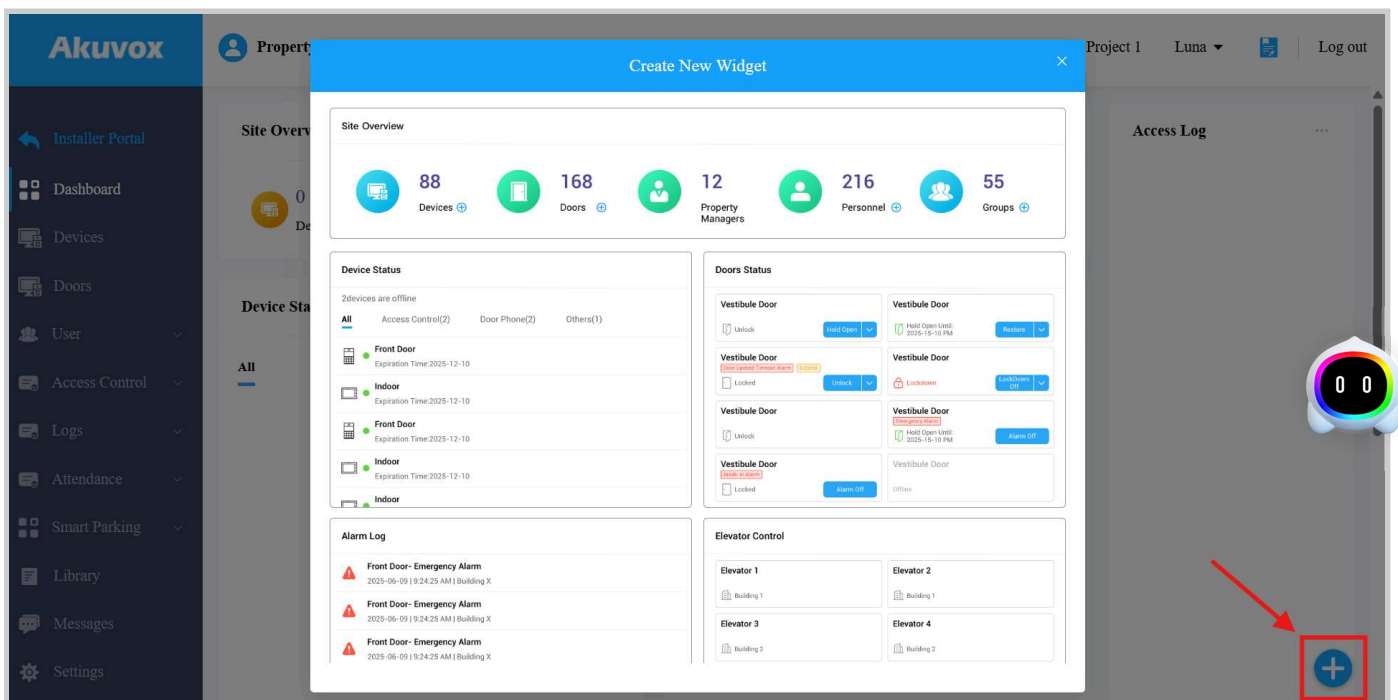
Building A





Add Components

1. Click + in the lower-right corner.
2. Click the desired component to add it. The same components can be added repeatedly.

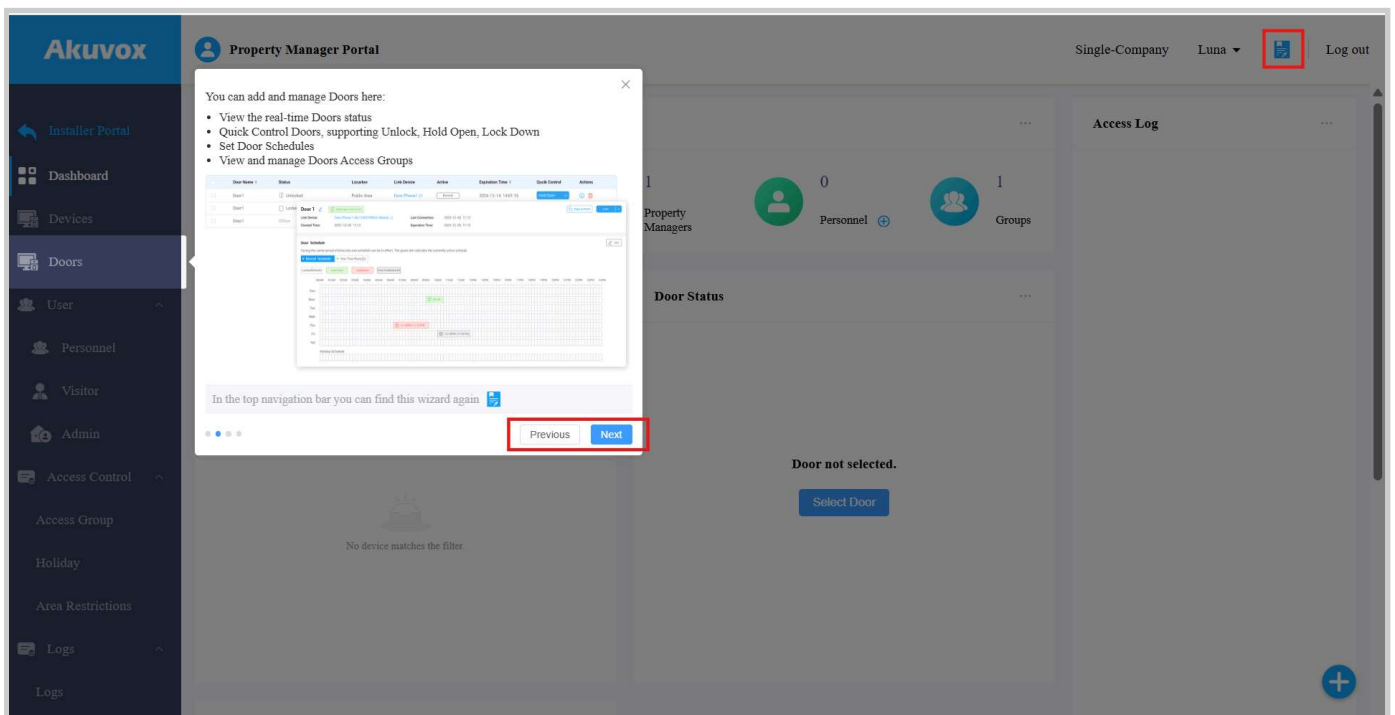


Wizard

Wizard guides you through adding devices, companies, administrators, groups, and personnel, and setting up access control and attendance. It will pop up when you log in to the platform. (For installer accounts, the Wizard will display when clicking  of the target project.)

Click **Previous** and **Next** to switch between the introductions to the specific modules.

If you want to check the guidance after closing it, click  in the upper-right corner.



Building Management

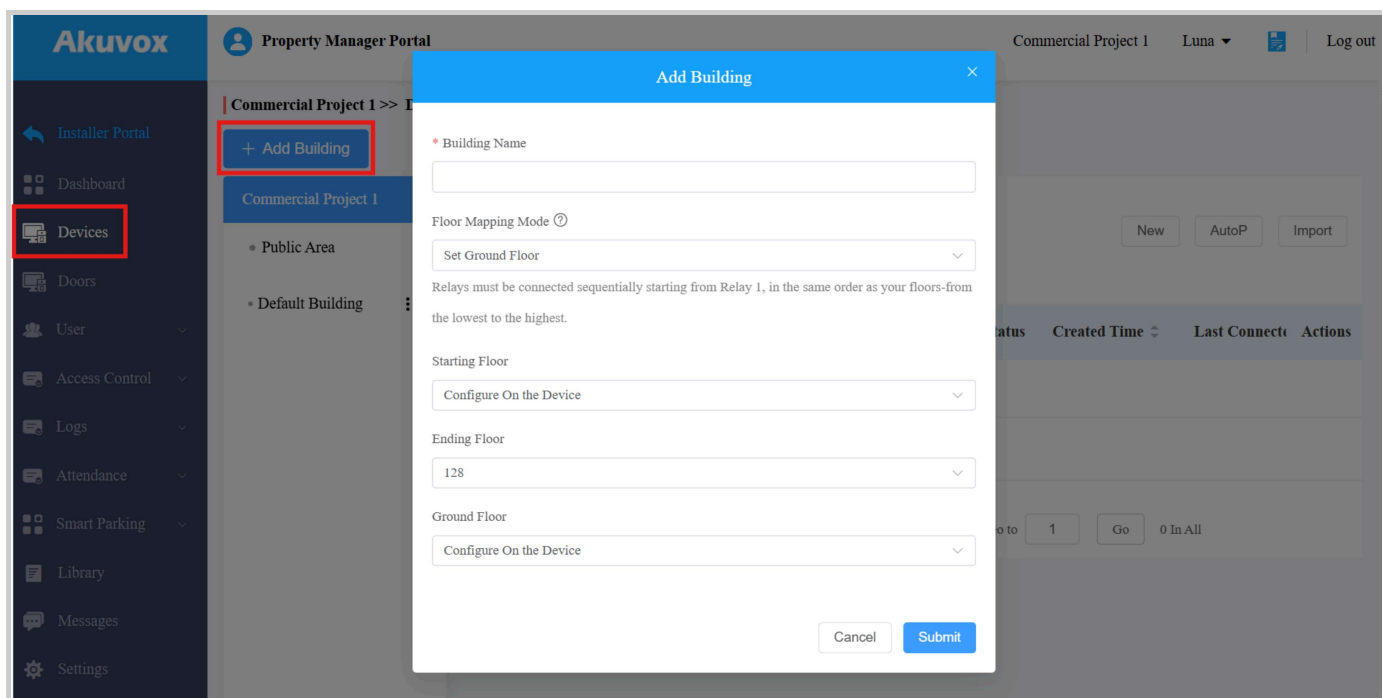
ONLY when the **Elevator Control** feature is enabled for the project, will building settings be available.

ONLY installers can add, edit, and delete buildings.

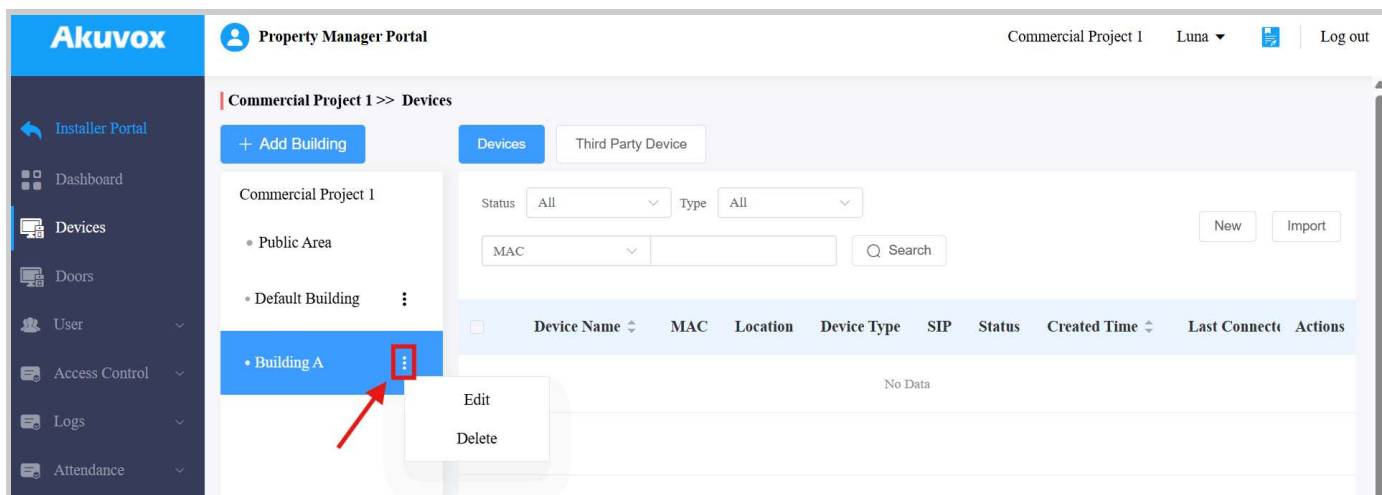


1. Click **Devices > +Add Building**.
2. Name the building.
3. The remaining settings are for Akuvox **EC33 Elevator Control**. If this device is not deployed in your project, you can skip these settings and submit directly.

To learn more about **Floor Mapping Mode** configuration, click [here](#).



4. Click  next to the desired building to edit its settings or delete it.



Group Management

You can add and modify groups.

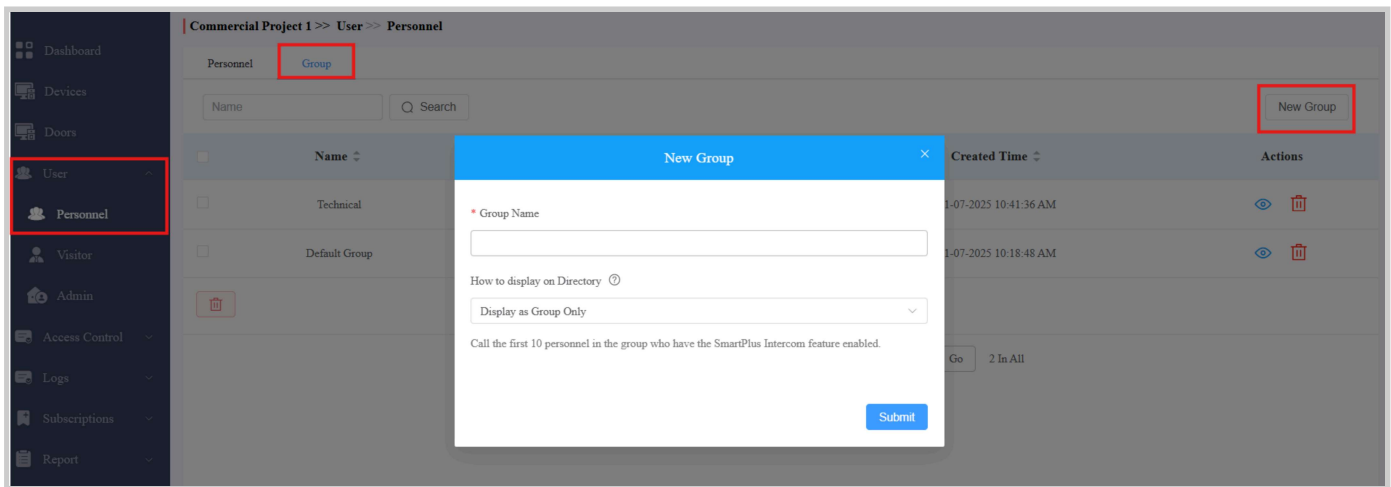
Add a Group

1. Click **User > Personnel > Group > New Group**.
2. Name the group.



3. Set the directory display on the door phone's directory screen. Specific models support this feature. See the note below.

- **Do not Display:** Neither display the group nor the personnel in it.
- **Display as Group Only:** The default option. Only display the group name. When selected, the first 10 personnel with the SmartPlus Intercom feature enabled will be called.
- **Display Personnel Only:** Personnel will all be displayed, but not the group name.



4. Click Submit.

Compatible models and versions(or higher):

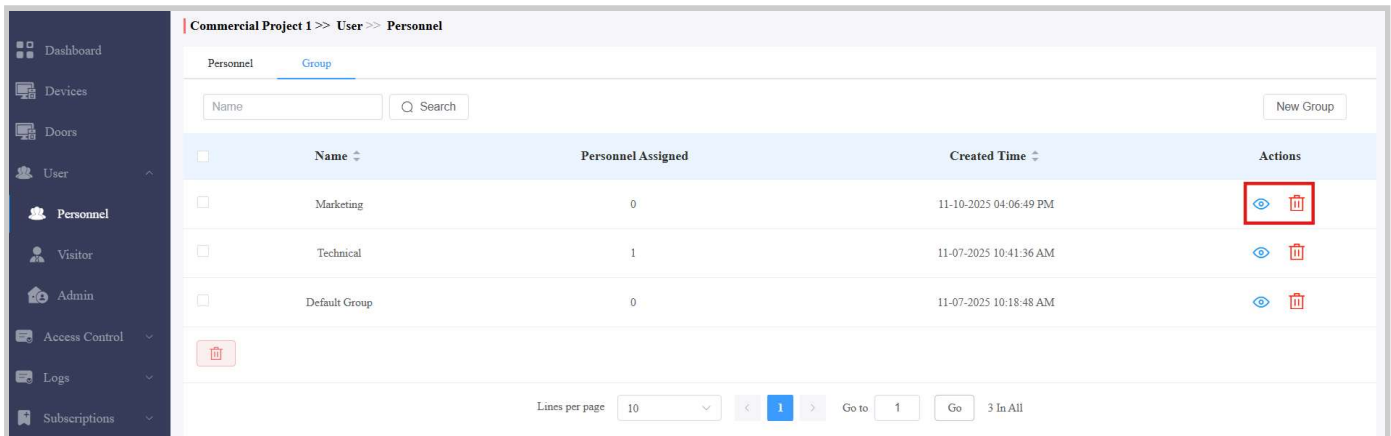
- X912: 912.30.11.49
- X915 V2: 2915.30.10.211
- X916: 916.30.10.222
- S539: 539.30.10.231
- S535: 535.30.10.233
- S532: 532.30.10.211
- R29: 29.30.10.314
- R28V2: 228.30.10.231
- E16V2: 216.30.10.208



Edit/Delete a Group

1. Click **User > Personnel > Group**.

2. Click  to view the detailed information and modify the group; click  to delete it.



Commercial Project 1 >> User >> Personnel

Personnel Group

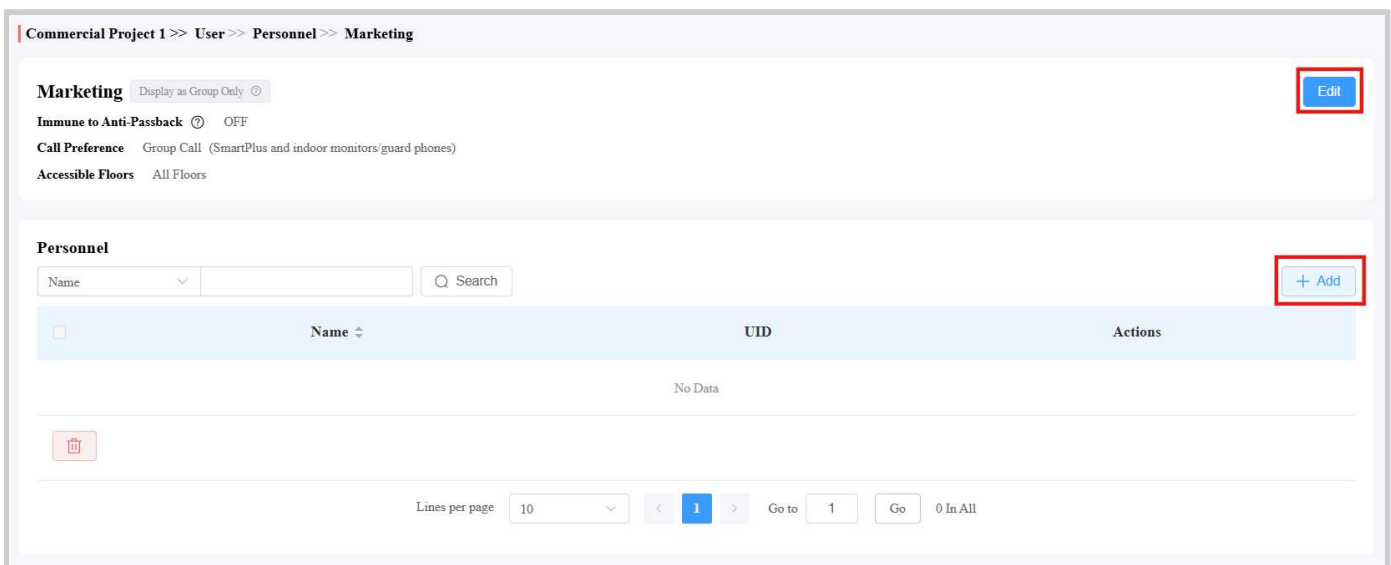
Name Search New Group

	Name	Personnel Assigned	Created Time	Actions
☐	Marketing	0	11-10-2025 04:06:49 PM	 
☐	Technical	1	11-07-2025 10:41:36 AM	 
☐	Default Group	0	11-07-2025 10:18:48 AM	 

Lines per page 10 < 1 > Go to 1 Go 3 In All

3. On the group info interface, you can:

- Click **+Add** to add users to the group.
- Click **Edit** to change the group settings.



Commercial Project 1 >> User >> Personnel >> Marketing

Marketing Display as Group Only OFF

Immune to Anti-Passback OFF

Call Preference Group Call (SmartPlus and indoor monitors/guard phones)

Accessible Floors All Floors

Personnel

Name Search + Add

	Name	UID	Actions
No Data			

Lines per page 10 < 1 > Go to 1 Go 0 In All

- Check the access groups applied to the group.
- Click **+Add** to add an access group.



	• X916: 916.30.10.222 • S539: 539.30.10.231 • S535: 535.30.10.233 • S532: 532.30.10.211 • R29: 29.30.10.314 • R28V2: 228.30.10.231 • E16V2: 216.30.10.208
Call Preference	Sequence Call: You can set three sequence call numbers, the numbers will receive calls in order. Group Call: The first 10 personnel with the SmartPlus receive the call.
Call Type	Set which devices receive calls from the door phone. For example, Indoor Monitors/Guard Phones with SmartPlus. Indoor monitors or guard phones receive the call first and forwards to users' SmartPlus Apps.
Immune to Anti-passback	When enabled, the personnel in this group will not be affected by Anti-passback rules.
Accessible Floors	• This setting works with the Akuvox elevator control system. The group can take the elevator to their accessible floors. • Set whether to choose All Floors. ◦ If not, specify the buildings and accessible floors from the dropdown menu. • Click here to view how to set up the elevator control.

Personnel Management

You can add personnel one by one or in a batch to the project.



Add Personnel One by One

1. Click **User > Personnel > New Personnel**.
2. Enter the user information and set up permissions.

See descriptions of each item in the chart below.

Item Name	Description
Profile Picture	Click Edit to upload the profile picture. Format: .jpg/.jpeg/.bmp/.png; Max picture size: 10MB resolution: 300×300. You can also choose the system default profile.
First Name/Last Name[The mandatory option]	The username.
UID	The UID. If you leave it empty, the system will generate a default UID.
Group	Assign the user to a group. Or, click +New Group to create a new group.
Job Title	The user's job title.
Email	The user's email address. SmartPlus App login credentials will be generated if the user can use the SmartPlus Intercom feature.
Mobile Number	The user's mobile phone number. Select the right area code and enter the number.
Language	All notifications sent to the user will display in the selected language.
Assigned Device	You can assign an indoor monitor/a guard phone to the user. When visitors call the user from a door phone, the device will ring.

Set Valid Time	Limit the user from opening doors and using the SmartPlus App within the specified time. This setting has the highest priority over other permission settings.
SmartPlus Intercom Feature	Disabled by default. If enabled, the user is allowed to use the SmartPlus App. This is a premium feature. Turning it on/off will incur additional billing.
Landline Service	• Available when SmartPlus Intercom Feature is enabled. • It enables communication between mobile phone and landline intercom devices. • When enabled, enter the landline number.
Call Type	When the SmartPlus Intercom Feature is enabled, set the call type as follows: • SmartPlus and indoor monitors/guard phones: When a user makes a call to the personnel on a door phone, the personnel's mobile phone, indoor monitors or guard phones will receive the call. • Indoor monitors/guard phones with SmartPlus: When a user makes a call to the personnel on a door phone, the personnel's mobile phone, indoor monitors/guard phones will receive the call. If the call is not answered, it will be made to the SmartPlus App.
Display in Directory	Enabled by default. Set whether to display the user's name in the directory list.
Privileges	• Create QR Code: Disabled by default. Set whether to allow the user to create the temporary QR code with their SmartPlus App. • First Credential in Permission: Enabled by default. Set whether the user can use their credentials to keep the door closed. • Lockdown Bypass: Enabled by default. Set whether to allow the user to open the door if it is locked down. NOTE: Specific models and versions(or higher) support Lockdown Bypass. • X912: 912.30.12.22 • X915V2: 2915.30.10.619 • X916: 916.30.10.508 • R29: 29.30.10.507 • R28V2: 228.30.11.6



- R20: 320.30.11.206
- E16V2: 216.30.11.107
- S539: 539.30.10.507
- S535: 535.30.11.8
- A08: 108.30.11.110
- A01/A02: 101.30.11.12
- A03: 103.30.11.6
- A095: 95.30.10.203
- A094: 92.30.11.8

3. Click **Next** to set up the user's credentials.

See description of each item in the chart below.

New Personnel

✓

Basic Information

2

Access Methods

You can set credentials here or set it later in detail page.

PIN

RF Card

Face ID

Use Profile Picture as Face ID

Fingerprint ?

Not Enrolled

License Plate

License Plate

UHF Card ?

☐ Set Valid Time

< Back

Cancel

Submit

Item Name

Description

PIN	2~8-digit PIN code.
RF Card	1~16 characters that can contain 0~9 and A~F.
Face ID	Upload the user's front-facing picture for facial recognition If you have uploaded a clear profile picture, you can also skip this step by clicking Use Profile Picture as Face ID .
Fingerprint	Enroll the fingerprint with the Akuvox fingerprint reader ACR-100
License Plate	Enter the number that a third-party LPR camera can identify.
UHF Card	Enter the card code that the Akuvox device ACR-CRP12 can identify.
Set Valid Time	Set when the vehicle can enter and exit the parking lot.

Note

- The license plate is used for [Smart Parking](#).
- If you have filled in both the License Plate and the UHF Card, the cloud will ONLY issue the UHF card code to the door phone.

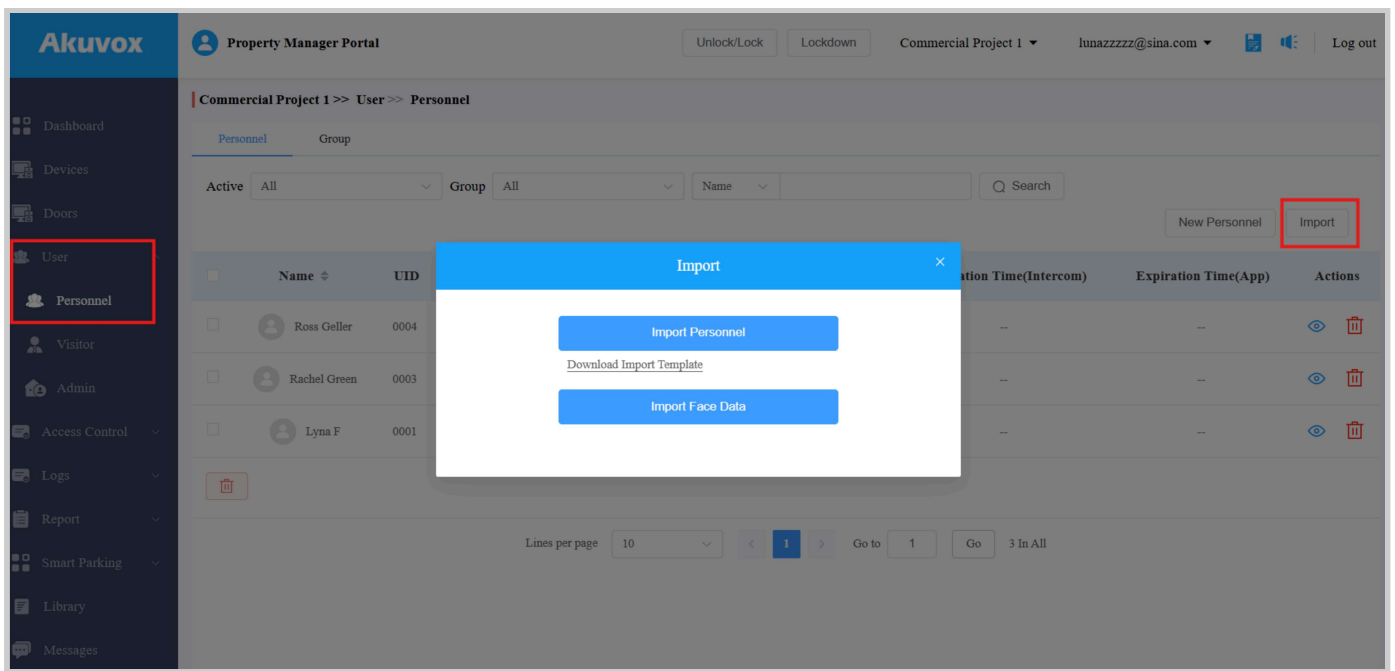
4. Submit the setting.

Add Personnel in a Batch

You can import a batch of personnel data to the project for quick setup.

1. Click **User > Personnel > Import**.
2. Click **Download Import Template**.
3. Click **Import Personnel** to upload the file after editing it, and click **Import Face Data** to upload the face photos. Please follow the upload instructions in the pop-up window.





In the template, you can see the instructions by moving the mouse cursor to a specific column.

See the description of each item in the chart below.

A	B	C	D	E	F	G	H	I	J	K
Group	FirstName	LastName	UID	Job Title	Email	MobileNumber	TelephoneCallingCode	Smartplus Intercom Feature	Landline Service	Landline Number
Sales	Steven	James	001	Sales	James@ak.com	1874577	1		0	

L	M	N	O	P	Q	R	S	T
CallType	RF Card	PIN	License Plate	UHF Card	Fingerprin	Access Group	IlFirst Credential In	Lockdown Bypass
0	FC11123	656897	WSD139					0

Column Name	Description
Group	The group of personnel. Separate multiple groups by ";"
First Name	The first name of the personnel.
Last Name	The last name of the personnel.
UID	Assign a unique ID to the personnel.
Job Title	The job title of the personnel.
Email	The email address of the personnel. It is used to rec emails.
Mobile Number	The mobile phone number of the personnel.
Telephone Calling Code	The telephone code for phone calls. For example, the coc States.



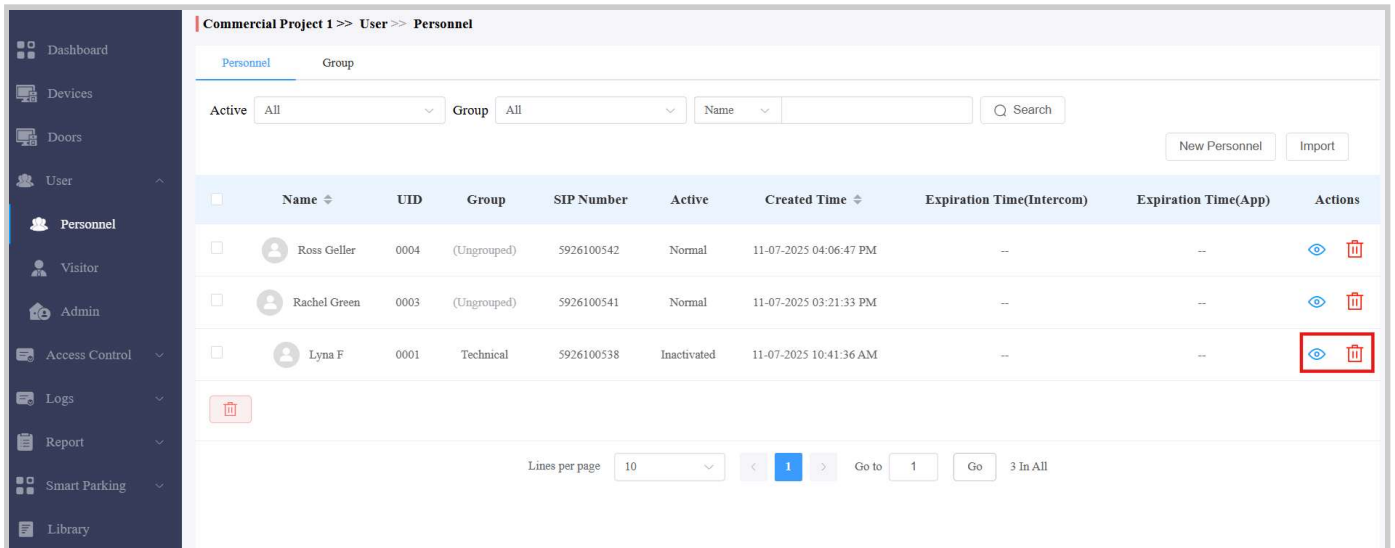
SmartPlus Intercom Feature	If enabled, the user is allowed to use the SmartPlus App. 0: Disabled; 1: Enabled.
Landline Service	Landline Service enables communication between telephone intercom devices. 0:Off; 1:On.
Landline Number	Enter the landline number when the landline service is active.
Call Type	Set which devices can receive a call. For example, if you select 0, the SmartPlus App will receive calls from the indoor monitor or the guard phone. 0: SmartPlus and indoor monitors/guard phones; 1: Phone and indoor monitors/guard phones; 2: SmartPlus and indoor monitors/guard phones, with phone as backup; 3: Indoor monitors/guard phones with SmartPlus as backup; 4: Indoor monitors/guard phones with phone as backup; 5: Indoor monitors/guard phones with SmartPlus as backup.
RF Card	The RF card code is used to open doors. If one user has multiple codes, separate the codes by ";".
PIN	The PIN code is used to open doors. The length should be 4-8 digits.
License Plate	Fill in the license plate information, multiple plate codes separated by ";". add up to 5 codes.
UHF Card	Fill in the UHF card code, multiple plate codes separated by ";". add up to 5 codes.
Access Group ID	Assign the access_group ID to the user.
First Credential In	Enabled by default. Set whether the user can use their first credential to open the door. 0:Off; 1:On.
Lockdown Bypass	Enabled by default. Set whether the user can open the door during lockdown. 0:Off; 1:On.



Edit Personnel

After adding the personnel, you can edit and delete them on the **User > Personnel** interface.

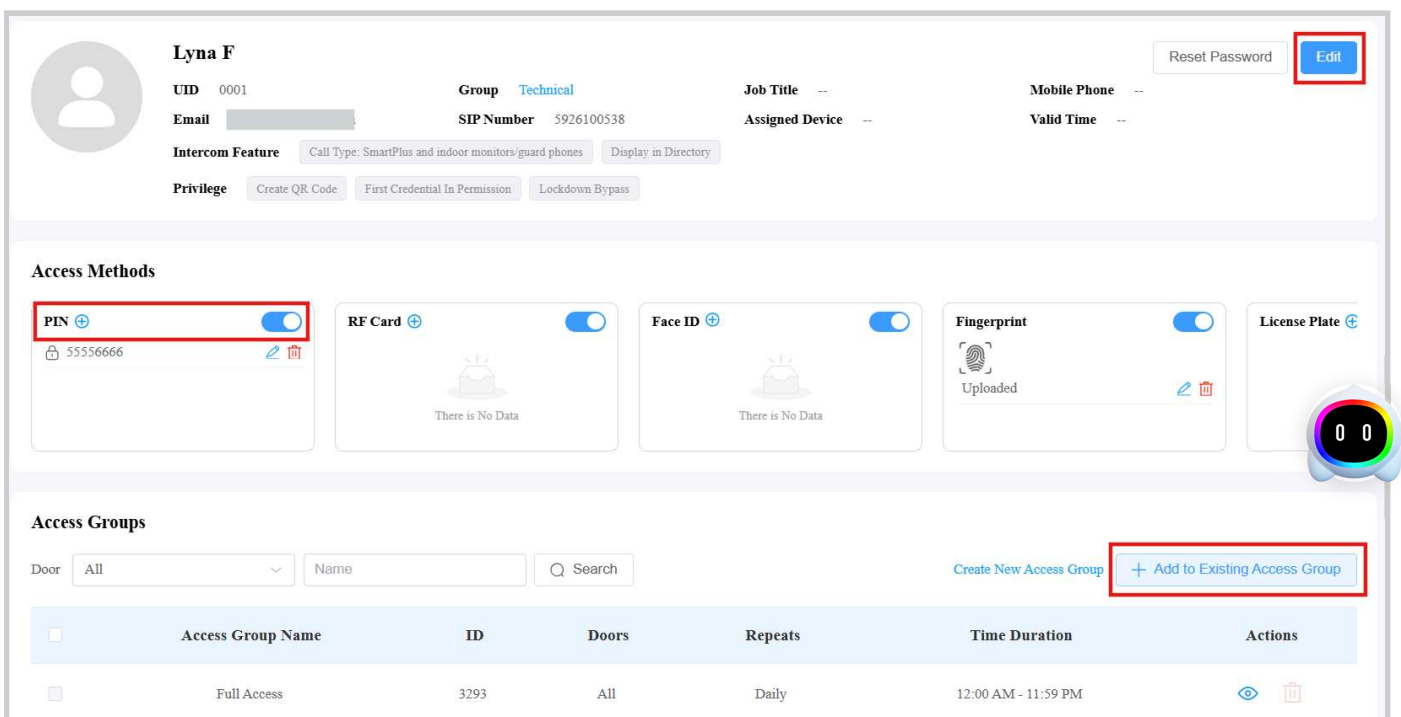
- Click  to delete the personnel.
- Click  to view and edit the personnel's information.



Name	UID	Group	SIP Number	Active	Created Time	Expiration Time(Intercom)	Expiration Time(App)	Actions
Ross Geller	0004	(Ungrouped)	5926100542	Normal	11-07-2025 04:06:47 PM	--	--	 
Rachel Green	0003	(Ungrouped)	5926100541	Normal	11-07-2025 03:21:33 PM	--	--	 
Lyna F	0001	Technical	5926100538	Inactivated	11-07-2025 10:41:36 AM	--	--	 

On the information interface, click **Edit** to modify the account settings.

- Toggle access methods' switch to turn them on/off.
- Click  to add specific access methods.
- Click  to check access groups applying to the user.
- Click **+Add to Existing Access Group** to add an access group.



Lyna F
UID 0001 Group **Technical** Job Title -- Mobile Phone --
Email [redacted] SIP Number 5926100538 Assigned Device -- Valid Time --
Intercom Feature: Call Type: SmartPlus and indoor monitors/guard phones Display in Directory
Privilege: Create QR Code First Credential In Permission Lockdown Bypass

Access Methods

PIN  
55556666  

RF Card  

There is No Data

Face ID  

There is No Data

Fingerprint  

Uploaded  

License Plate 

Access Groups

Door: All Name: Search: [Create New Access Group](#) **+ Add to Existing Access Group**

Access Group Name	ID	Doors	Repeats	Time Duration	Actions
Full Access	3293	All	Daily	12:00 AM - 11:59 PM	 

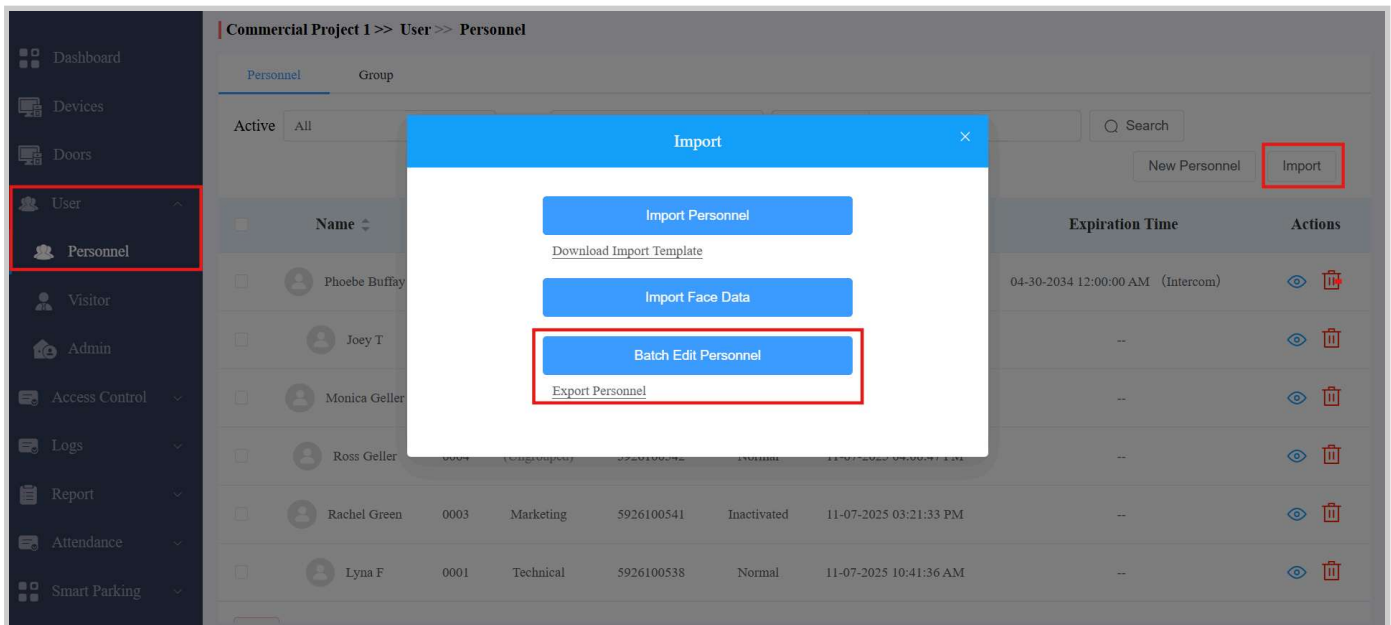
Edit Personnel in a Batch

You can export the personnel file, edit it, and import it to make a bulk modification.

Note

ONLY with a **PM** account will this feature be available.

1. Click **User > Personnel > Import**.
2. Click **Export Personnel**.
3. Click **Batch Edit Personnel** to upload the file after editing it.



	A	B	C	D	E	F	G	H	I	J
1	Group	FirstName	LastName	UID	Job Title	Email	MobileNumber	TelephoneCallingCode	Smartplus Intercom Feature	Landline Service
2	Technic	Lyna	F	0001					1	0
3	Marketi	Rachel	Green	0003				1	1	0

K	L	M	N	O	P	Q	R	S	T	U
Landline Number	CallType	RF Card	PIN	License Plate	UHF Card	Fingerprint	Access Group ID	First Credential In	Lockdown Bypass	SIP Number
0	0		55556666			C53C6000528!		1	1	5926100538
	0		1234567	UHD223			3320	1	0	5926100541

Note

- Group name cannot be modified.
- The email address of an account linked to multiple sites cannot be modified.
- Adding or updating an email address will reset the SmartPlus App login password. The new login credentials will be sent to the new email address.

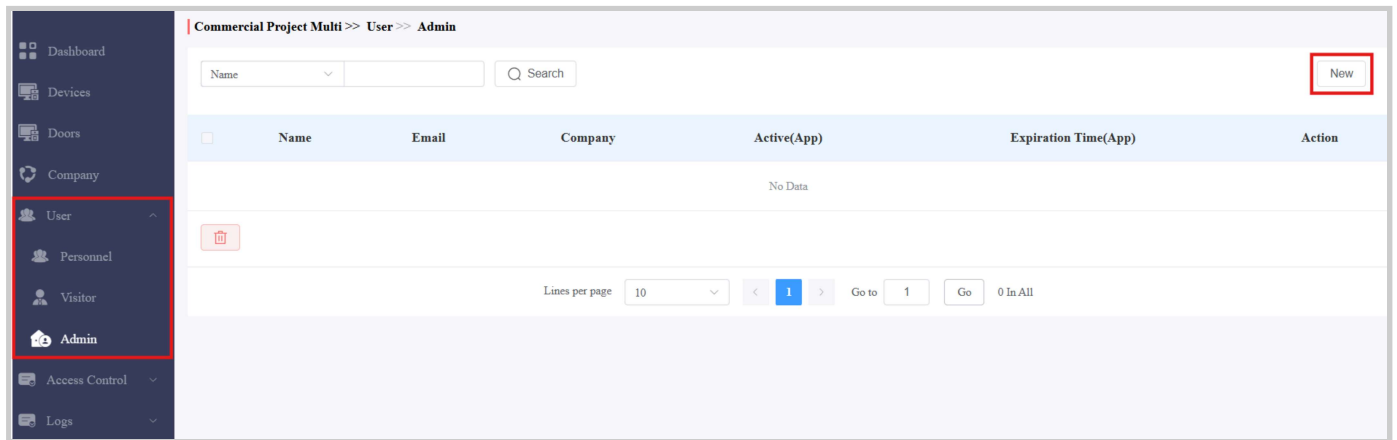


- Access credentials can be added but not modified.

Administrator Management

You can create administrator accounts, with which users can log in to the Smart Access Administrator platform to manage companies, personnel, access groups, etc.

1. Click **User > Admin > New**.



2. Set up the account. See the descriptions of each item in the chart below.



Dashboard

Devices

Doors

Company

User

Personnel

Visitor

Admin

Access Control

Logs

Report

Smart Parking

Library

Messages

Settings

Role

Company Administrator

* Company ?

* Group

* First Name

* Last Name

* Email

Mobile Number

+1

Admin APP Service

Privileges

First Credential In Permission ?

Lockdown Bypass ?

Submit

Item Description:

Item Name	Description
Company	Select the company managed by the administrator.
Group	Select the group of the administrator.
First Name/Last Name	Enter the name of the administrator.
Email	The email is used to log into the SmartPlus Admin web.
Mobile Number	Enter the mobile phone number if the administrator v App login. Note: Select the right area code. Or, the number will
Admin App Service	Set whether the administrator can use the SmartPlus

Landline Service	- Available when Admin App Service is enabled. - It enables communication between mobile phone devices. - Enter the number of the administrator's phone w
Call Type	Available when Admin App Service is enabled. SmartPlus: The SmartPlus App and indoor monit Phone: The phone and indoor monitor will receiv SmartPlus with phone as backup: SmartPlus and called first, then the forwarded phone number if
Privileges	First Credential In: Disabled by default. Set whe credentials to keep the door open. Lockdown Bypass: Disabled by default. Set whe door when it is locked down. NOTE: Specific models and versions(or higher) supp - X912: 912.30.12.22 - X915V2: 2915.30.10.619 - X916: 916.30.10.508 - R29: 29.30.10.507 - R28V2: 228.30.11.6 - R20: 320.30.11.206 - E16V2: 216.30.11.107 - S539: 539.30.10.507 - S535: 535.30.11.8 - A08: 108.30.11.110 - A01/A02: 101.30.11.12 - A03: 103.30.11.6 - A095: 95.30.10.203 - A094: 92.30.11.8



After adding the accounts, you can click  to change the settings and reset the account's password.

Commercial Project Multi >> User >> Admin

Name

☐	Name	Email	Company	Active(App)	Expiration Time(App)	Action
☐	Admin A		Company 1	--	--	 

Lines per page: 10 1 1 In All

Mobile Number

+1

Admin APP Service ☐

Privileges

First Credential In Permission ☐ ?

Lockdown Bypass ☐ ?

Device Management

- With the PM account, you can view and edit the device's settings, but NOT add or delete a device.
- With the installer account redirecting from the installer portal, you can add, edit, and delete devices.

Add a Single Device

1. On the **Devices** module, click **New** on the right.
2. Enter the device's information. See the item description in the chart below.



Akuvox Property Manager Portal

Add Device

Device Type: Multi-tenants Doorphone

* MAC:

Network Group: Network 1

* Device Name:

Allow user to monitor this device? ☒

Door 1  ☒

* Door Name: Door1

DTMF Code: #

Door Control

* Controlled Relay

Cancel Submit

New AutoP Import

Last Connected Time Actions

11-07-2025 02:18:26 PM

Note

Adding A095 requires its version to be 95.30.10.125 or higher.

Regardless of what type of device it is, the device type, MAC address, network group.

No.	Field Name	Description
1	Device Type	Select your device type. - ONLY when the Elevator Control feature is enabled, v available. - To add an EC33, its firmware version should be 33.30 - It can ONLY be added to the public area of specific b
2	MAC	Type in the device's MAC address.
3	Network Group	Select the network group. You can select the same network devices are deployed in the same local network. (In t Note: Do not select the same network group if the d the same local area network(in this case, communicate vi communication failure.
4	Device Name	Name the device to distinguish it from others.

To add a door phone or an access control terminal, the following options should be

1	Allow users to monitor this device	- You can decide whether users can view the monitoring video on indoor monitors. It is enabled by default. - When disabled, the Monitor button on users' SmartPhone will not see the video during a call with an intercom device.
2	Door Name	Enter the door name, which can be the device location.
3	DTMF Code	Enter the DTMF code for the door access.
4	Controlled Relay	Specify the relay that is connected to the door lock. For A095, select Door1~4 or AUX OUT1~4.
5	Entry Reader	The reader controls the entry door. Internal Reader: Use the device's built-in reader. For example, users swipe cards on a built-in card reader to open doors. Wiegand A ~ D: Use a device connected to the door phone's Wiegand ports. For example, users swipe cards on a Wiegand card reader to open doors. RS485 A ~ D: Use a device connected to the door phone's RS485 ports. For example, users swipe cards on an RS485 card reader to open doors. NOTE: When the controlled relay is selected Door(A095), A095 has 8 reader interfaces that can be connected for Wiegand and RS485.
6	Exit Reader	The reader controls the exit door. Internal Reader: Use the device's built-in reader. For example, users swipe cards on a built-in card reader to open doors. Wiegand A ~ D: Use a device connected to the door phone's Wiegand ports. For example, users swipe cards on a Wiegand card reader to open doors. RS485 A ~ D: Use a device connected to the door phone's RS485 ports. For example, users swipe cards on an RS485 card reader to open doors. NOTE: When the controlled relay is selected Door(A095), A095 has 8 reader interfaces that can be connected for Wiegand and RS485.
7	Access Method	Available when Internal Reader is selected as the Entry Reader. Select specific unlock methods to open doors. For example, select RF Card for Door 2, when users enter PIN codes on the device and vice versa. The following models with specific firmware versions or higher support the Access Method feature.



S539	539.30.10.118	R25A	25.:
S535	535.30.10.233	R25K	25.:
S532	532.30.10.117	R27	227
X916	916.30.10.216	R28	28.:
X915 V1	915.30.10.128	R28 V2.0	228
X915 V2	2915.30.10.106	R29	29.:
X912	912.30.10.225	A094	92.:
X910	2910.30.10.240	A095	95.:
E16 V2	216.30.10.69	A05V2	205
E18	18.30.10.205	A08	108
R20 V5.0	320.30.10.125		

Note: If the **SmartPlus Homepage** or **SmartPlus Talking p** icons will not appear on the app home page.

8	RS485_Address	Available when RS485 is selected as the Entry Reader/Ex Select the RS485 address ranging from 0 to 127.
9	Exit Button	Input A ~ D: Select it when the input is connected to an e door. NOTE: When the controlled relay is selected Door(A095) , the label on the device.
10	Door Sensor Connect To	Select the input port that is connected to a door sensor. It breaks in forcibly or if the door-opening time exceeds a li • Input A ~ D: This setting is effective for models r  • Magnetic A ~ D(A094): This setting is only effective i • DPS1~4: This setting is available when the controlled corresponds to the label on the device.
11	Door Status Indicated	Use the relay or the door sensor(connected to the device

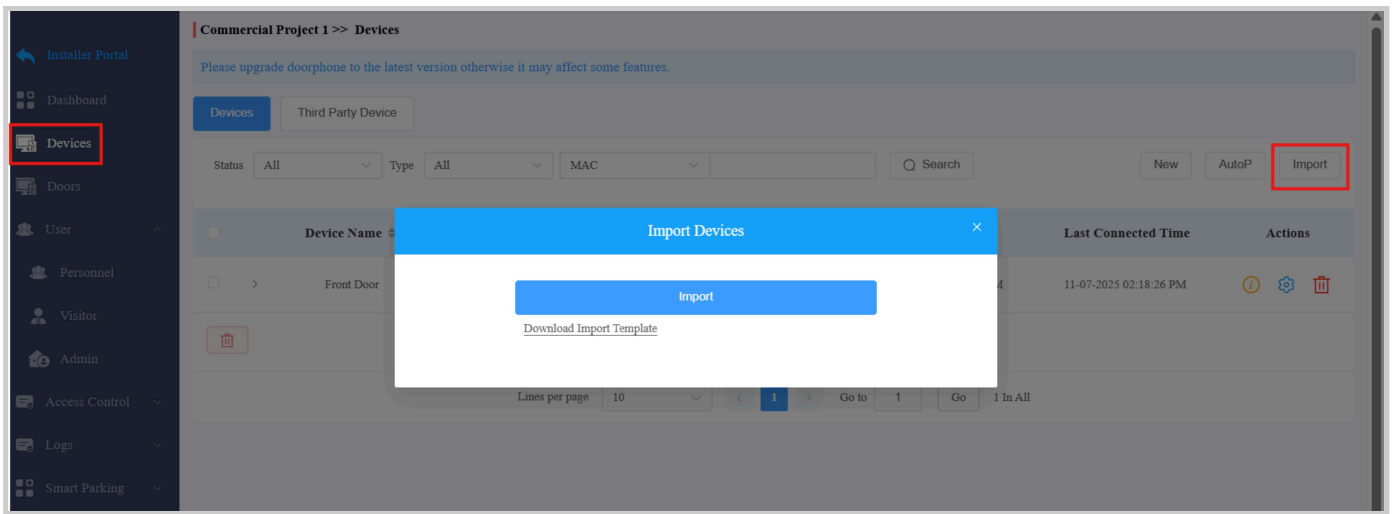
	By	
12	Add Door	Add doors when the device is connected to more than one

To add an indoor monitor/guard phone, the following options should be additional		
1	Arming Function	When enabled, the arming icon will be available on users' disarming.
2	Companies	Available when the device type is guard phone. - The All Companies option is checked by default, indicating Apps and/or indoor monitors used) in all companies with directory screen. - When unchecked, select specific companies. Note: R49 with version 49.30.10.43 or higher supports this
3	Belongs To	You can link the device to a specific user. - The device will be displayed as contacts on the personnel screen. - When initiating a group call to the personnel on a guard phone called. - When calling the personnel on an access control terminal on the Call Type settings. - When initiating a sequence call to the personnel on a guard phone based on the Sequence Call settings.
4	Relay	This option is for indoor monitors. Turn on or off the device

Add Devices in a Batch

1. On the **Devices** module, click **Import** on the right.
2. Download and open the template. Click **Import** after editing the file.





In the template, enter the device name, type, and MAC address as instructed.

A	B	C	D	E	F	G	H
Device	Device Name, Device Type, MAC; Values of device type are as below: 0 = Multi-tenants Doorphone 1 = Single-tenant Doorphone 2 = Indoor Monitor 3 = Guard Phone 50 = Access Control Multiple devices separate by semicolon(;) eg. Front Indoor, 2, A41003FFFFFF;Garage, 1, A41002FFFFFF						

Edit/Delete Devices

On the **Devices** module,

- Click  to view the device information.
- Click  to change the device's settings. Please note that if you change the device's MAC address, the related door logs, call histories, motion alerts, alarm records, and captures will be cleared.
- Click  to delete it.
- Click  to display the configured door.



Please upgrade doorphone to the latest version otherwise it may affect some features.

Devices Third Party Device

Status All Type All MAC Q Search New AutoP Import

	Device Name	MAC	Device Type	SIP	Status	Created Time	Last Connected Time	Actions
☐	Front Door	0C110518CC4D				11-07-2025 10:32:27 AM	11-07-2025 02:18:26 PM	

Door Name	Controlled Relay	Status	Active	Expiration Time	Action
Door1 Free	Relay A	Locked	Normal	--	

Apart from the basic settings, including device name and network group, you can set up alarm settings.

Alarm Setting

Door Held Open Alarm ? ☐

Break-in Alarm ? ☐

- **Door Held Open Alarm:** Available when **Door Status** is configured. This feature allows the device to sound an alarm when the door-opening time exceeds a certain limit.
 - **Door Opened Timeout:** Set the door-opening time beyond which the alarm will be triggered.
- **Break-in Alarm:** The feature allows the device to sound an alarm when the door is opened abnormally.

Note

- Click [here](#) to view the models supporting the Break-in Alarm feature.
- The following device models with specific firmwares or higher support the Door Held Open Alarm feature:

Model	Version	Model	Version
A08	108.30.10.108	R29	29.30.10.314
A01/A02	101.30.10.106	R28 V2	228.30.10.218
A03	103.30.10.108	R25	25.30.10.117



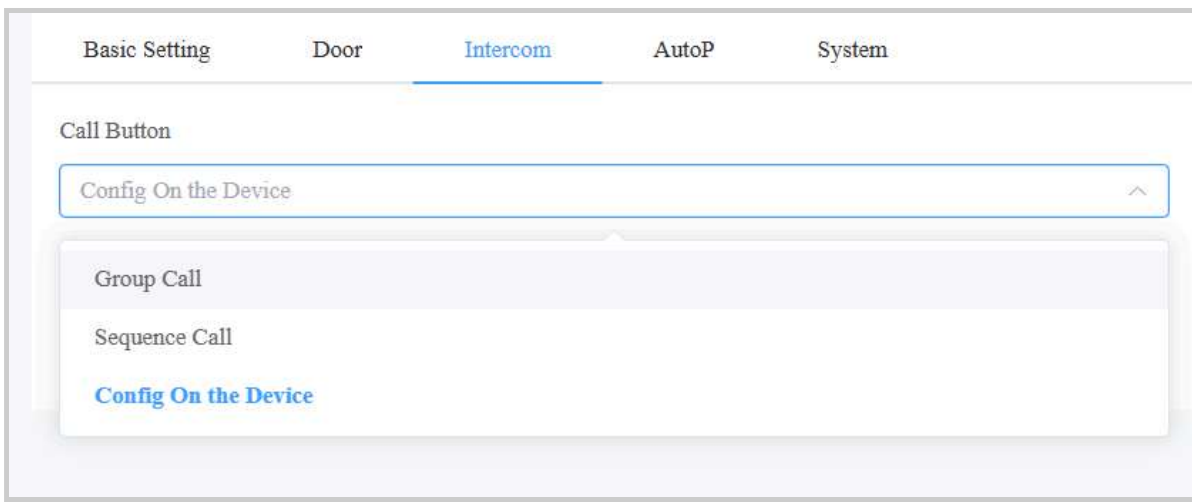
A05 V2	205.30.10.119	E18	18.30.10.236
A094	92.30.10.112	E16 V2	216.30.10.208
A095	95.30.10.125	X910	2910.30.11.28
X912	912.30.11.49	X915 V2	2915.30.10.211
S532	532.30.10.211	S535	535.30.10.233
E12 V2	312.30.11.18	S539	539.30.10.249
X916	916.30.10.224	R20 V5	320.30.10.226

Modify the Call Button Setting

If the device type is **Single-tenant Doorphone**, the intercom setting is available. This allows you to set up the call type and issue contact information to single-button door phones, such as R20A, E12, and X910.

1. Click  of the target door phone.
2. Select **Intercom**.
3. Select the desired call type.
 - **Group Call:** The default option. When visitors press the call button, the first 10 indoor monitors/guard phones and personnel's SmartPlus Apps/landline numbers will receive the call simultaneously.
 - **Sequence Call:** When visitors press the call button, calls will be made in sequence to the selected indoor monitors/guard phones, and personnel's SmartPlus Apps/landline numbers. You can set up 3 groups, each with up to 5 options.
 - **Call Timeout(Sec):** 5~60 seconds. The interval between calling each group of numbers.
 - **Config on the Device:** Select this option when the device's on-premise configuration takes precedence.





Basic Setting Door **Intercom** AutoP System

Call Button

Config On the Device

Group Call

Sequence Call

Config On the Device

4. Click Submit.

Note

- The [directory_display_mode](#) should be set to **Display as Personnel** when adding/editing the group. Otherwise, it will fail to make a call by pressing the call button.
- The following models with specific versions or higher have fixed this problem.
 - E12: 312.30.11.27
 - R20A: 320.30.11.214
 - X910: 2910.30.11.51

Modify Elevator Control Setting

When the device is an elevator control device, configure additional elevator control settings when edit it.

Click [here](#) to view the setting details.



Basic Setting

Elevator Control

AutoP

System

Controlled Floors

☒ All Floors

Trigger Device

Add

Floor Schedule

The floor button will be enabled during the configured schedule.

Floor

Q Search

New

Floor	Schedule	Actions
No Data		

Device Remote Maintenance

You can manage devices remotely in terms of automatic provisioning(AutoP), reboot, reset, connection type selection, etc.

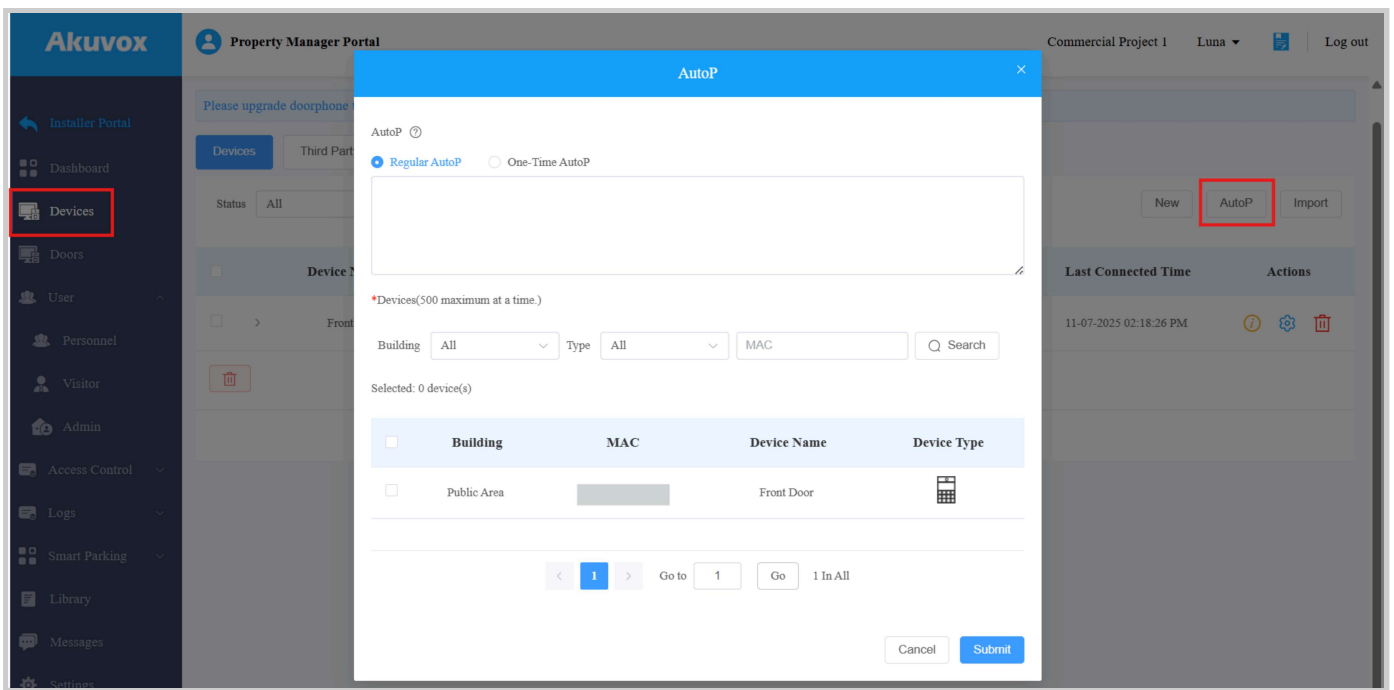
Batch AutoP

With an installer account, you can select multiple devices to perform AutoP.

If you are a project manager, simply skip this part.

1. Click **Devices > AutoP**.
2. Select **Regular AutoP** or **One-Time AutoP**. The latter only implements the command once.
3. Enter the command.
4. Check the desired device(s).





5. Click Submit.

AutoP on a Specific Device

On the **Devices** module, click  of the target device. Or, click  and click **Settings**.

- Click **AutoP** and enter the commands. Click **One Time AutoP** and enter the commands if you just want to implement the AutoP once.

- Click **System**, where you can select the connection type, reboot or reset the device, and access the device's web interface by clicking **Remote Control**.

Basic SettingDoorAutoPSystem

Connection Type

TCP

Reboot

Reboot

Reset

Reset

Remote Control

Remote Control

Submit

Back>>

Note

- The Auto-provisioning command can be exported out of the devices.
- You can download the following templates:
 - Door Phones: <https://knowledge.akuvox.com/docs/autop-commandsdoor-phones>
 - Indoor Monitors: <https://knowledge.akuvox.com/docs/autop-commandsindoor-monitors-1>
- Duplicate commands will not be retained.

Check Third-party Devices

You can check the information on the Salto locks on the **Devices** module.

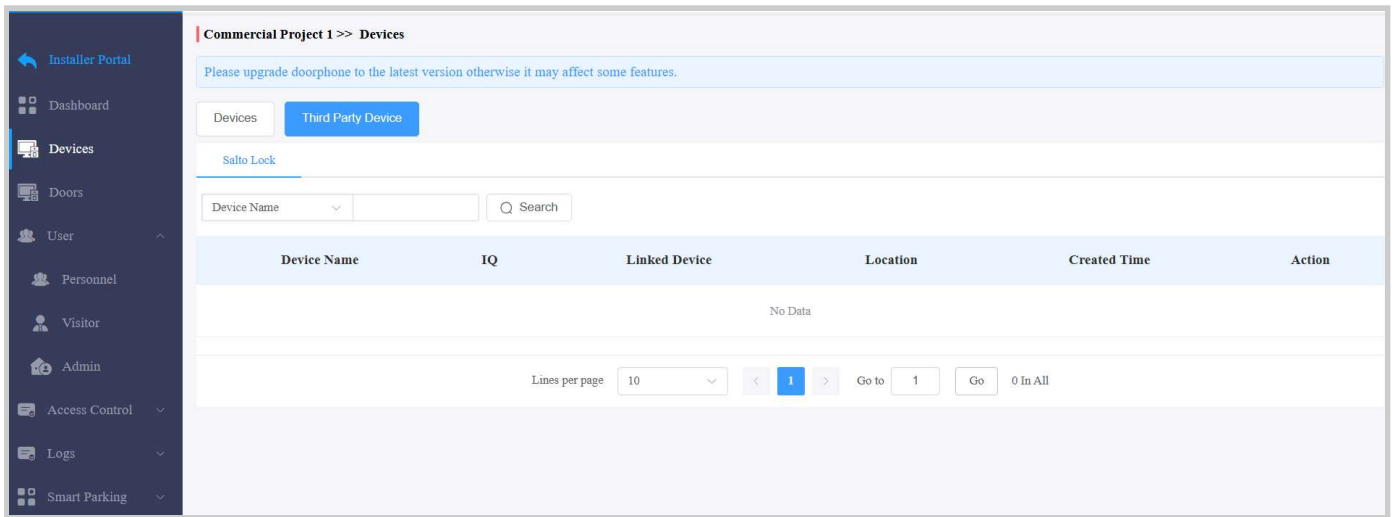
Note

As an installer, you can refer to the article [Integration with Salto Lock](#) for adding and assigning the Salto locks.



Click **Third-Party Devices**.

In the Action column, you can click  to view the lock's detailed information and click  to modify the lock's name.



Door Management

You can manage doors through quick control and schedules.

Access Control Priority Levels:

- **Quick Control:** ONLY available for **project managers**. Highest priority. Control doors even if they are in the state preconfigured by the **Door Schedule**. For example, if a door is set to hold open from 8 AM to 12 PM daily, you can close the door at any time via quick control.
- **One-Time Runs:** The second-highest priority. Only one schedule can be active per day, and one-time runs take precedence over Routine Schedules and Holidays. For instance, if a door is set to hold open for one-time runs on a holiday, users can open it during the holiday.
- **Holiday and Routine Schedule:** These have the lowest priority and will only be effective if there are no active One Time Runs or Quick Control adjustments.

Compatible Devices	
Features	Models and Versions(or Higher)
Check door status	• X912: 912.30.12.22 • X915V2: 2915.30.10.619 • X916: 916.30.10.508

	• R29: 29.30.10.507 • R28V2: 228.30.11.6 • R20: 320.30.11.206 • E16V2: 216.30.11.107 • S539: 539.30.10.507 • S535: 535.30.11.8
Door quick control	
Door schedule	• A08: 108.30.11.110 • A01/A02: 101.30.11.12 • A03: 103.30.11.6 • A095: 95.30.10.203 • A094: 92.30.11.8

Door Quick Control

On the **Doors** module, you can check the added doors, their status, location, expiration time, etc.

As a **PM**, you can perform door quick control(**unlock, hold open, and lock down**). Installers have no such permission.

Door Activation Status:

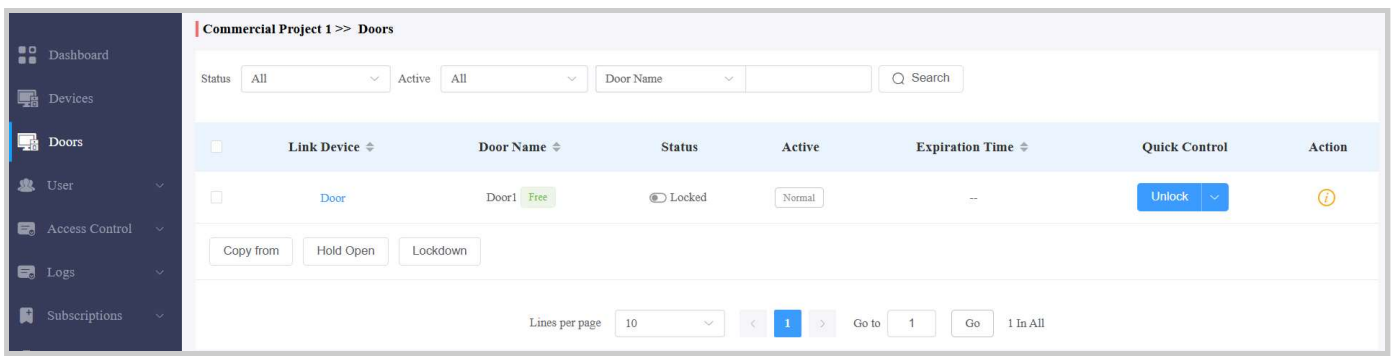
- **Free:** The door is free to use.
- **Expired/Unsubscribed:** The door is not activated or expires, which limits the cloud services, including issuing credentials to open the door, remotely configuring and managing the door phone, and reporting door logs to the cloud.

Door Status: The door status is configured when you(installer) add [the device](#).

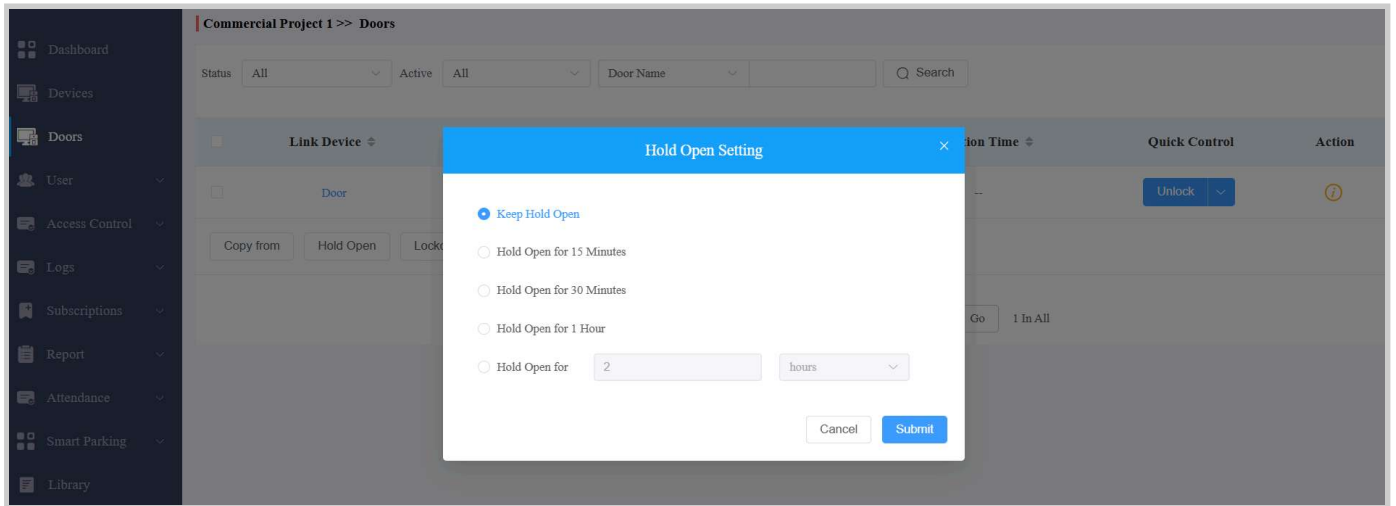
 Locked /  Unlocked : The door status is not configured.

 Locked /  Hold Open : The door status is indicated by the input status.





When setting the door to remain open, select the time. To close it while it is open, click **Restore**.



Lockdown

The lockdown feature keeps the door locked. It can be used to keep threats out in dangerous situations.

Doors under lockdown cannot be opened by common access methods, such as users' credentials and the exit button.

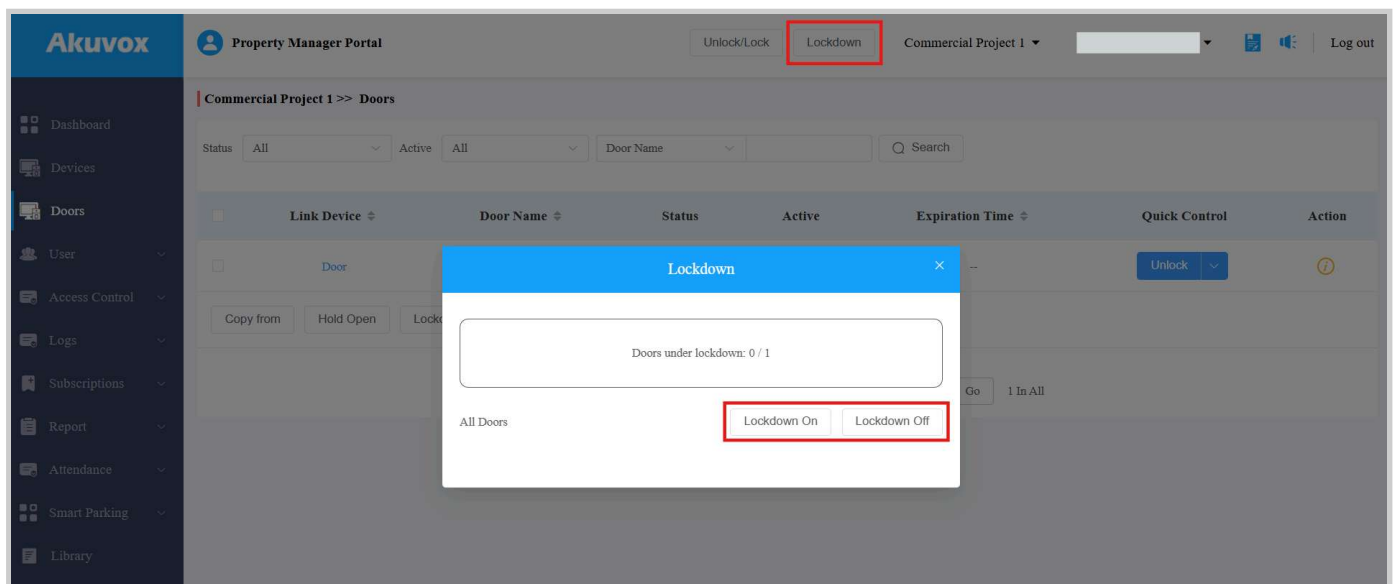
Compatible models and versions(or higher):

Model	Version	Model	Version
R29	29.30.10.404	X910	2910.30.11.28
R28V2	228.30.10.231	X912	912.30.11.107
R25	25.30.10.117	X915V2	2915.30.10.420
R20	320.30.11.30	E16 V2	216.30.10.208



A08	108.30.11.8	A01/A02	101.30.10.206
A03	103.30.10.204	A094	92.30.10.205
A095	95.30.10.125	S539	539.30.10.507
X916	916.30.10.508	S535	535.30.11.8

1. Click **Lockdown** at the top of any interface. This button is only available for project manager accounts.
2. Click **Lockdown On** to lock all doors; click **Lockdown Off** to release all doors.



If users try to open doors in lockdown, devices with screens will display “Property Under Lock” and announce an alarm; devices without screens will shine a blue indicator light and announce an alarm.

Switch Lockdown for a Specific Door

You can check the doors’ lockdown status and turn on/off lockdown for a specific door by clicking **Lockdown On/Off** in the **Quick Control** column.



Commercial Project 1 >> Doors

Status All Active All Door Name Q Search

☐	Link Device	Door Name	Status	Active	Expiration Time	Quick Control	Action
☐	Door	Door1 Free	Lockdown	Normal	--	Lockdown Off	i

Copy from Hold Open Lockdown

Lines per page 10 < 1 > Go to 1 Go 1 In All

Modify Door Settings

1. On the **Doors** module, click i of the desired door.

Commercial Project 1 >> Doors

Status All Active All Door Name Q Search

☐	Link Device	Door Name	Status	Active	Expiration Time	Quick Control	Action
☐	Door	Door1 Free	Locked	Normal	--	Unlock	i

Copy from Hold Open Lockdown

Lines per page 10 < 1 > Go to 1 Go 1 In All

2. Click **Copy to/from** to copy the configuration data to/from another door.

Commercial Project 1 >> Doors >> Info

Door - Door1 Locked

Link Device: Door() - Relay A **Active:** Normal **Last Connection:** 01-04-2026 02:15:32 PM

Created Time: 01-04-2026 02:12:32 PM **Expiration Time:** --

Copy to/from Unlock



Copy to/from ×

! If the door is already configured, using "Copy to/from" will overwrite its current configuration.

*** Target Data**

☐ Door Schedule

*** Action**

☒ Copy to
 ☐ Copy from

*** Door**

Cancel Submit

Door Schedule

The Door Schedule refers to a timetable for doors to change to a preset state at specific times.

It supports two repeat modes:

- **Routine Schedules:** The schedule repeats every week.
- **One-Time Runs:** Set the daily or weekly schedule that repeats during a defined period.

Routine Schedules

1. On the **Doors** module, click  of the desired door.

- Dashboard
- Devices
- Doors**
- User
- Access Control
- Logs
- Subscriptions
- Report

Commercial Project 1 >> Doors

Status All Active All Door Name

Q Search

	Link Device	Door Name	Status	Active	Expiration Time	Quick Control	Action
☐	Door	Door1 Free	Locked	Normal	--	Unlock	

Copy from
Hold Open
Lockdown

Lines per page 10
< 1 >
Go to 1 Go 1 In All



00

2. To set up a routine schedule, click **Edit** on the **Door Schedule** section.

3. Select the door mode that will be highlighted.

- **Hold Open**: The door remains open during the scheduled time.
- **First Credential In**: The door remains open during the scheduled time after users use their credentials for the first time.
- **Lockdown**: The door remains closed during the scheduled time.

4. Hold and drag your mouse cursor to select a time block.

While setting up the schedule, you can:

- Click **Copy from** to copy a schedule from a configured door.
- Click **Undo** to withdraw the configuration.
- Click **Clear** to remove the configuration.

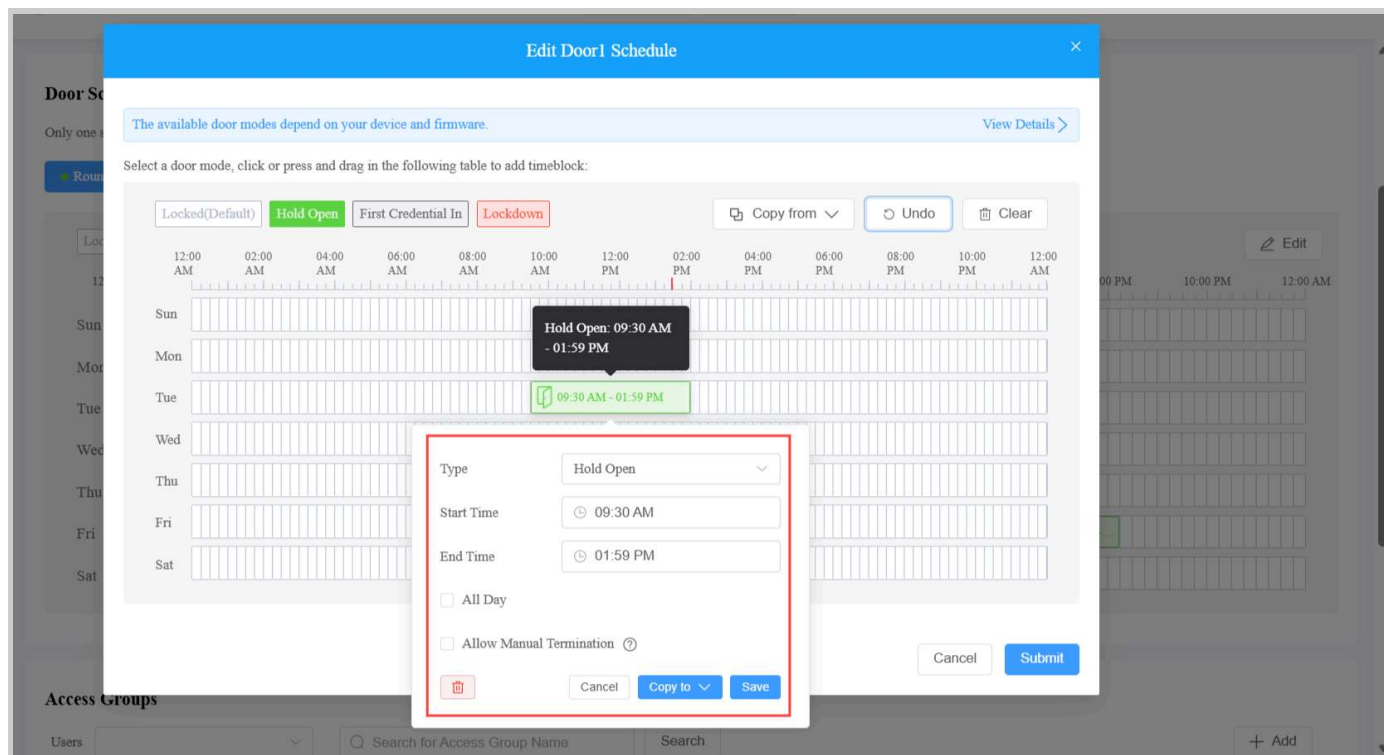
5. Set up the time block by clicking it.

You can:

- Change the type.
- Select the start time and end time.
- Check **All Day**.
- Check **Allow Manual Termination**. If enabled, users with the first credential in permission can close the door when it is held open.



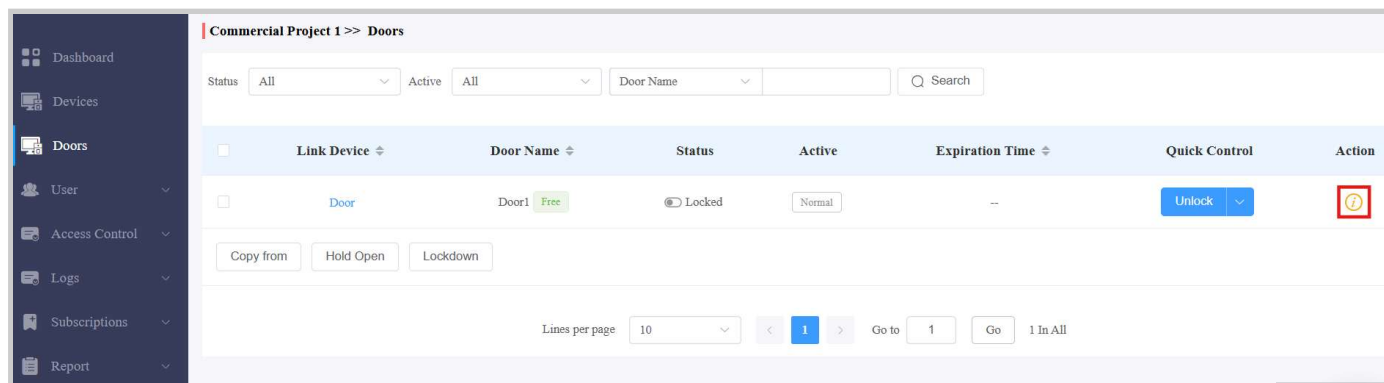
- Copy the schedule to the whole week, weekend, or weekdays by clicking **Copy to**.



6. Save the setting and submit the schedule.

One-Time Schedules

1. On the **Doors** module, click  of the desired door.



2. Select **One-Time Runs** on the Door Schedules section.
3. Click **+Add One-Time Runs**.
4. Name the schedule.
5. Specify the schedule's effective time.



6. Select the **Repeats** mode: Daily or Weekly.

7. Select the door mode that will be highlighted.

- **Hold Open**: The door remains open during the scheduled time.
- **First Credential In**: The door remains open during the scheduled time after users use their credentials for the first time.
- **Lockdown**: The door remains closed during the scheduled time.

Door Schedule

Only one schedule can be active at a time.

● Routine Schedule

Add One Time Runs

* Name

Effective Time

Start Date To End Date

Repeats

Daily

The available door modes depend on your device and firmware. [View Details](#)

Select a door mode, click or press and drag in the following table to add timeblock:

Locked(Default) **Hold Open** First Credential In Lockdown

12:00 AM 02:00 AM 04:00 AM 06:00 AM 08:00 AM 10:00 AM 12:00 PM 02:00 PM 04:00 PM 06:00 PM 08:00 PM 10:00 PM 12:00 AM

Daily

07:45 AM - 01:29 PM

Undo Clear

Cancel Submit

8. Set up the time block by clicking it.

You can:

- Change the type.
- Select the start time and end time.
- Check **All Day**.
- Check **Allow Manual Termination**. If enabled, users with the first credential in permission can close the door when it is held open.
- Copy the schedule to the whole week, weekend, or weekdays by clicking **Copy** to.



Door Schedule

Only one schedule can be active at a time.

Add One Time Runs

* Name

Effective Time

Start Date End Date

Repeats

Daily

The available door modes depend on your configuration.

Select a door mode, click or press and drag in the calendar to set the time.

Locked(Default) **Hold Open** Fire

Type: Hold Open

Start Time: 07:45 AM

End Time: 01:29 PM

☐ All Day

☐ Allow Manual Termination ?

Cancel Copy to Save

Undo Clear

06:00 PM 08:00 PM 10:00 PM 12:00 AM

Daily 07:45 AM - 01:29 PM

Cancel Submit

9. Save the setting and submit the schedule.

Access Group Management

Access Group allows you to create an inventory of ready-made access control schedules, which can be readily pulled out and applied for the door access control, targeting specific groups and personnel.

Create an Access Group

1. Click **Access Control > Access Group > +New Access Group**.

Akuvox Property Manager Portal

Unlock/Lock Lockdown Commercial Project 1

Commercial Project 1 >> Access Control >> Access Group

Users Doors Name Search

+ New Access Group

Name	ID	Users	Doors	Repeats	Time Duration	Actions
Full Access	3293	All	All	Daily	12:00 AM - 11:59 PM	
Access Group 1	3314	All	All	Daily	09:00 AM - 06:00 PM	

Lines per page 10 Go to 1 Go 2 In All

2. Name the group.
3. Select the repeat mode: Daily, Weekly, or Never.
4. Enable/disable **Holiday Exemption**. This decides whether the users in the access group can open doors during [holiday schedules](#). Specific devices support this feature.

Compatible models and versions(or higher):

- X912: 912.30.12.22
- X915V2: 2915.30.10.619
- X916: 916.30.10.508
- R29: 29.30.10.507
- R28V2: 228.30.11.17
- R20: 320.30.11.206
- E16V2: 216.30.11.107
- S539: 539.30.10.507
- S535: 535.30.11.8
- A08: 108.30.11.110
- A01/A02: 101.30.11.12
- A03: 103.30.11.6
- A095: 95.30.10.203
- A094: 92.30.11.8

Commercial Project 1 >> Access Control >> Access Group >> New

* Name

Access Group 2

Access Schedule When access group works?

Repeats

Daily

Click or press and drag in the following table to edit timeblock:

Select All DayUndoClear

12:00 AM	02:00 AM	04:00 AM	06:00 AM	08:00 AM	10:00 AM	12:00 PM	02:00 PM	04:00 PM	06:00 PM	08:00 PM	10:00 PM	12:00 AM
						09:00 AM - 06:00 PM						

☐ Holiday Exemption ⓘ

5. Select the door(s) to be opened. If **Custom** is selected, choose the door from the dropdown menu.

Doors Which doors are allowed?

☐ All ☒ Custom

6. Select users who are authorized to open the door.
- If **Custom** is selected, click **+Add** in the **Groups** section to select a group.
All users in the group will be granted permission to open the door.
 - Click **+Add** in the **Personnel** section to select a specific user.

Users Who can enter these doors?

☐ All ☒ Custom

Groups(2) ⓘ

Group Name

☐	Group Name	Actions
☐	Technical	Delete
☐	Default Group	Delete

Personnel(1)

Group Name

☐	Name	UID	Group	Actions
☐	 Rachel Green	0003	(Ungrouped)	Delete

7. Submit the setting.

Edit/Delete Access Groups

The system-generated default group cannot be edited or deleted.



- Click **Access Control > Access Group**.
- Click  to view the group's detailed information; click  to modify its settings; click  to delete it.

Holiday Access Control

You can define the holidays when personnel cannot open doors to enhance access control security.

Compatible models and versions(or higher):

Model	Version	Model	Version
X910	2910.30.11.28	R20V5.0	320.30.10.223
X912	912.30.11.49	R25	25.30.10.117
X915V2	2915.30.10.211	R29	29.30.10.314
X916	916.30.10.222	R28V2	228.30.10.218
S532	532.30.10.211	A08	108.30.10.108
S535	535.30.10.233	A01/A02	101.30.10.106
E18	18.30.10.236	A03	103.30.10.108
E16V2	216.30.10.208	A05V2	205.30.10.119
A094	92.30.10.112	A095	95.30.10.125
E12V2	312.30.11.18	S539	539.30.10.249

1. Click **Access Control > Holiday > New**.

The screenshot displays the Akuvox Property Manager Portal interface. On the left sidebar, the 'Access Control' menu is expanded, and the 'Holiday' option is highlighted. The main content area is titled 'Commercial Project 1 >> Access Control >> Holiday'. It features a search bar with a 'Search' button and a 'New' button in the top right corner. Below the search bar is a table with columns 'Name', 'Repeat by Year', and 'Actions'. The table is currently empty, displaying 'No Data'. At the bottom of the table, there are pagination controls showing '1' of '1' items.

2. Enter the holiday name.

3. You can set the **Working Hours** to allow authorized personnel to open doors.
When enabled, specify the time.
4. You can enable **Repeat by Year** to repeat the schedule every year.
5. Select the year and day(s) of the holiday schedule.

Commercial Project 1 >> Access Control >> Holiday >> New

* Holiday Name

Working Hours ⓘ

☐

Repeat by Year

☐

Year

2025

Jan

Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	01	02	03	04
05	06	07	08	09	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	01

Feb

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	01
02	03	04	05	06	07	08
09	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	01

Mar

Sun	Mon	Tue	Wed	Thu	Fri	Sat
23	24	25	26	27	28	01
02	03	04	05	06	07	08
09	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	01	02	03	04	05

Apr

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	31	01	02	03	04	05
06	07	08	09	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	01	02	03

May

Sun	Mon	Tue	Wed	Thu	Fri	Sat
-----	-----	-----	-----	-----	-----	-----

Jun

Sun	Mon	Tue	Wed	Thu	Fri	Sat
-----	-----	-----	-----	-----	-----	-----

Jul

Sun	Mon	Tue	Wed	Thu	Fri	Sat
-----	-----	-----	-----	-----	-----	-----

Aug

Sun	Mon	Tue	Wed	Thu	Fri	Sat
-----	-----	-----	-----	-----	-----	-----

6. Submit the setting.

Area Restrictions

This feature strictly controls users' entry and exit. Users can only enter and exit the specific area through the designated doors.

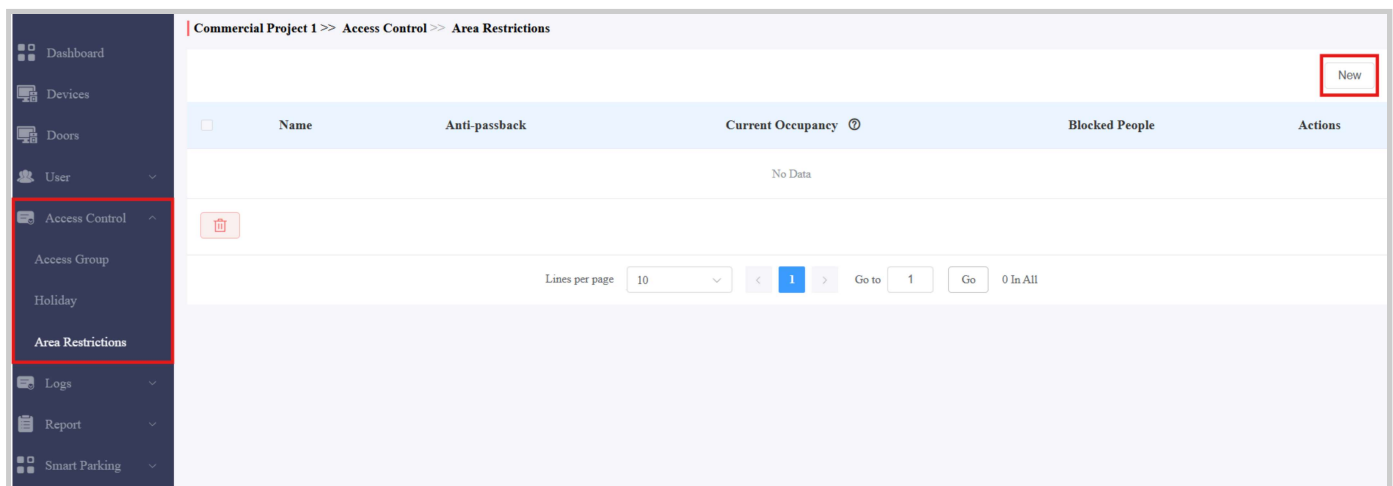
Compatible models and versions(or higher):

Model	Version	Model	Version
A08	108.30.10.108	R29	29.30.10.314
A01/A02	101.30.10.106	R28V2	228.30.10.218
A03	103.30.10.108	R25	25.30.10.117
A05V2	205.30.10.119	S539	539.30.10.231



A094	92.30.10.112	S535	535.30.10.233
A095	95.30.10.125	S532	532.30.10.211
X910	2910.30.11.28	E18	18.30.10.236
X912	912.30.11.49	E16V2	216.30.10.208
X915 V2	2915.30.10.211	E12V2	312.30.11.18
X916	916.30.10.222	R20V5	320.30.10.226

1. Click **Access Control > Area Restrictions > New**.



2. Enter the area name.
3. Select the entry and exit doors. With anti-passback disabled, there is no strict control over users exiting through the exit door. Users can exit through the entry door.
4. When the anti-passback feature is enabled, users must first enter and then exit the area through designated doors.

Note

- Anti-passback also prohibits users from entering the area by following others. Users can only use their credentials to open the entry and exit doors once respectively.



- For example, if the user follows someone else through the door, the next time he/she cannot swipe his/her card to open the Entry/Exit door.

a. Set the time when the anti-passback feature is effective.

b. Select the action taken by the door phone when the user tries to open the same entry or exit door twice.

-Deny Access: The user cannot open the door.

-Log violations only: The door can be opened, and the door opening will be recorded in the door log.

5. Set the **User Timeout** within which users cannot open the same door twice. Only after the time limit can users open the door again.

Commercial Project 1 >> Access Control >> Area Restrictions >> New

* Area Name

* Entry Doors

* Exit Doors

Anti-passback

☒

Schedule ?

Always

When Re-entry or Re-exit ?

☒ Deny Access ☐ Log violations only

User Timeout ?

1 hour

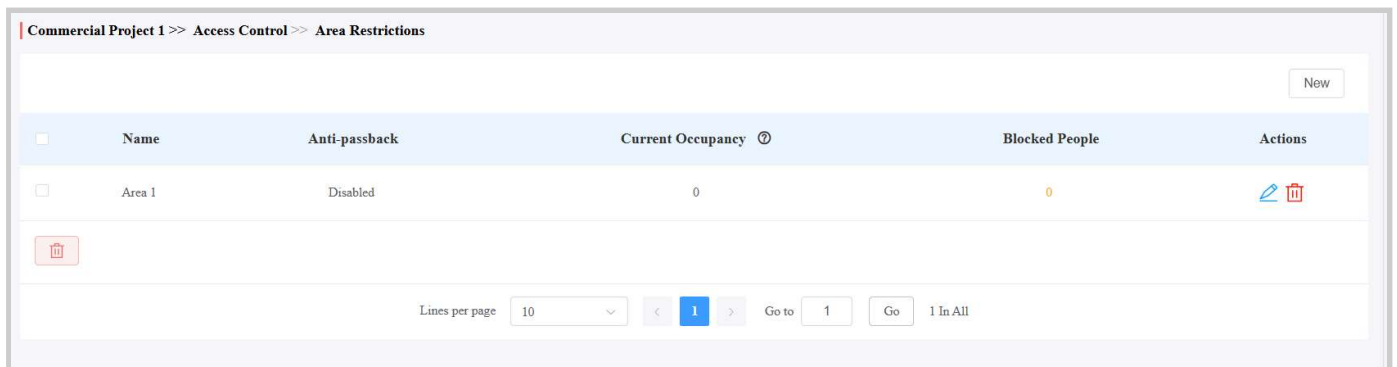
Submit



6. Submit the setting.

After creating the area restriction rule, you can check the current occupancy and blocked people.

- **Current Occupancy:** Display the number of personnel entering the area, only effective when the anti-passback feature is enabled.
- **Blocked People:** Display the number of personnel and couriers who are denied access in the area. It is only effective when the anti-passback feature is enabled and **Deny Access** is selected as the action for **When Re-entry or Re-exit**.



☐	Name	Anti-passback	Current Occupancy ⓘ	Blocked People	Actions
☐	Area 1	Disabled	0	0	 

Lines per page: 10 < 1 > Go to 1 Go 1 In All

Attendance

The attendance feature allows you to:

- set up independent attendance for each company;
- designate specific device relays as the attendance points;
- flexibly make timetables and schedule shifts;
- record leaves and attendance easily.

Note

Click [here](#) to view the feature configuration.



Visitor Management

You can set up access credentials for visitors and delivery personnel.

Access Credentials for Visitors

You can create temporary PIN codes along with QR codes for visitors, set the time when the credentials are valid, and select the door to be opened.

1. Click **User > Visitor > New**.

The screenshot shows the Akuvox Property Manager Portal. The left sidebar has a red box around the 'User' menu, which is expanded to show 'Personnel' and 'Visitor'. The 'Visitor' option is highlighted. The main content area is titled 'Akuvox Test3 >> User >> Visitor'. It has two tabs: 'Temp Keys' and 'Delivery Auth'. Below the tabs are filters for 'Validity' (All), 'Repeats' (All), 'Created By', 'Key', and 'Name', followed by a 'Search' button and a 'New' button (highlighted with a red box). Below the filters is a table with columns: Name, Key, QR Code, Validity Times Per Device, Repeats, Created By, Start Time, End Time, and Actions. The table is currently empty, showing 'No Data'. At the bottom, there is a 'Lines per page' dropdown set to 10, a pagination control showing '1' of 1 page, and a 'Go to' field with '1' and a 'Go' button. The status '0 In All' is shown at the bottom right.

2. Enter the visitor's name.
3. [Optional] Set a unique ID for the visitor.
4. Specify the time within which visitors can open doors by selecting the **Repeats** mode from **Daily**, **Weekly**, or **Never**. Daily and Weekly means the schedule will repeat every day and week.
5. Set the **Validity Times Per Device** when you select the **Never** Repeats mode. For example, if you enter 1 and check three door phones, the visitor can use the credential to open doors three times.
In other words, the validity times of credentials = Validity Times Per Device x The number of door phones selected.
6. Enter the visitor's email address in the Delivery Method to receive the temporary key.
7. Check the door(s) to be opened by the visitor.



* Name

ID Number

Repeats

* Begin Time

* End Time

* Validity Times Per Device

Email

* Door

Location	Device Name	MAC	Status	Door
Public Area	Front Door		●	☐ Door1 ☐ Door2

8. Click Submit.

After creating the temp key, you can

- check its details by clicking  and delete it by clicking .
- search for the desired key by its validity, repeat mode, who created the key, key value, and visitor name.
- print it out for the visitor. The QR code is generated with the visitor's name, the visited company, and the key.

Akuvox Test3 >> User >> Visitor

Temp Keys Delivery Auth

Validity Repeats Created By Key Name

☐	Name	Key	QR Code	Validity Times Per Device	Repeats	Created By	Start Time	End Time	Actions
☐	TEST	95428771		100	Never	Luna	13-01-2026 09:58:54 AM	27-01-2026 12:00:00 AM	  

On the temp key's information interface, you can click **View Door Logs** to check the door-opening record.

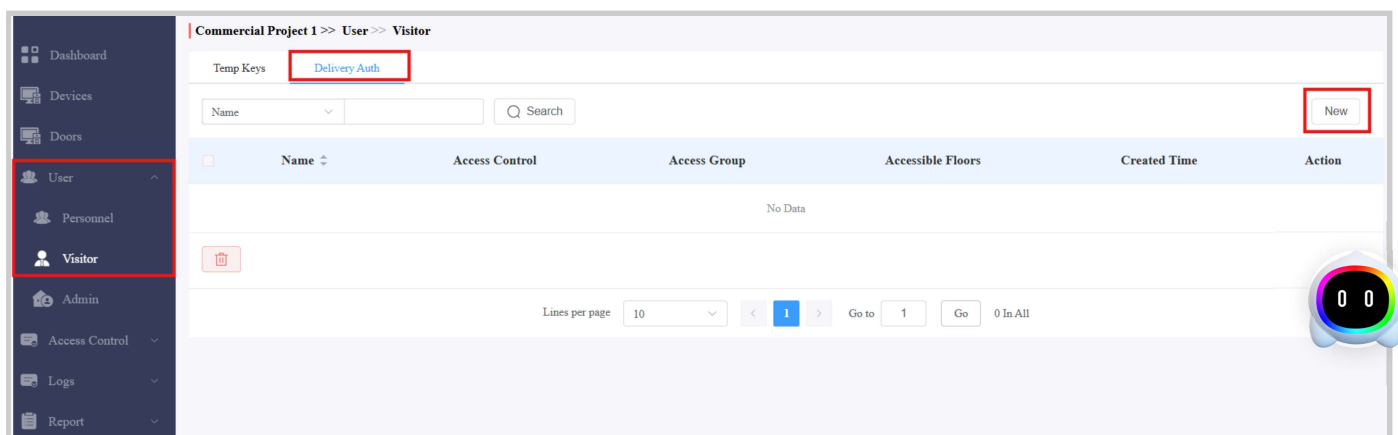
Company	Default Company
Name	Visitor 1
ID Number	--
Created By	
Key	92086420 View Door Logs
Repeats	Never
Validity Times Per Device	100
Start Time	11-10-2025 01:48:18 PM
End Time	11-30-2025 12:00:00 AM

QR Code


Access Credentials for Delivery Personnel

You can create PIN codes and RF card credentials for delivery personnel, with which they can access the designated place, such as a package room.

1. Click **User > Visitor > Delivery Auth > New**.



2. Enter the deliveryman's name.
3. Enter the PIN code and/or the RF card code. The PIN code should be within 2 to 8 digits, not starting with "9".

4. Set the accessible floors. The deliveryman can take lifts to the specified floors using access control credentials. You can select 10 floors in a building at a maximum. This feature works with the Akuvox EC33 lift controller.
5. Check the [schedule](#) for when the deliveryman can open the door. You can also click **New** to create a new schedule.

Commercial Project 1 >> User >> Visitor >> New Delivery Auth

* Name

PIN

RF Card

Accessible Floors
Please set the accessible floors for specific buildings.
 -

* Access Group New

Selected(0):

☐	Name	Door	Repeats	Time Duration
☐	Full Access	All Doors	Daily	12:00 AM - 11:59 PM
☐	Access Group 2	--	Daily	09:00 AM - 06:00 PM

6. Click Submit.

After creating the credential, you can modify it by clicking  and delete it by clicking .

Commercial Project 1 >> User >> Visitor

Temp Keys Delivery Auth

Name New

☐	Name	Access Control	Access Group	Accessible Floors	Created Time	Action
☐	Delivery	PIN:278932 RF Card:--	Full Access	--	11-10-2025 01:55:42 PM	 



Lines per page 1 In All



Muster Report

The muster report is used during emergencies, such as evacuations, to account for personnel. It tracks who is present during an evacuation and identifies missing

people.

ONLY project managers have permission to set this feature up.

Note

Click [here](#) to view the configuration details.

Smart Parking

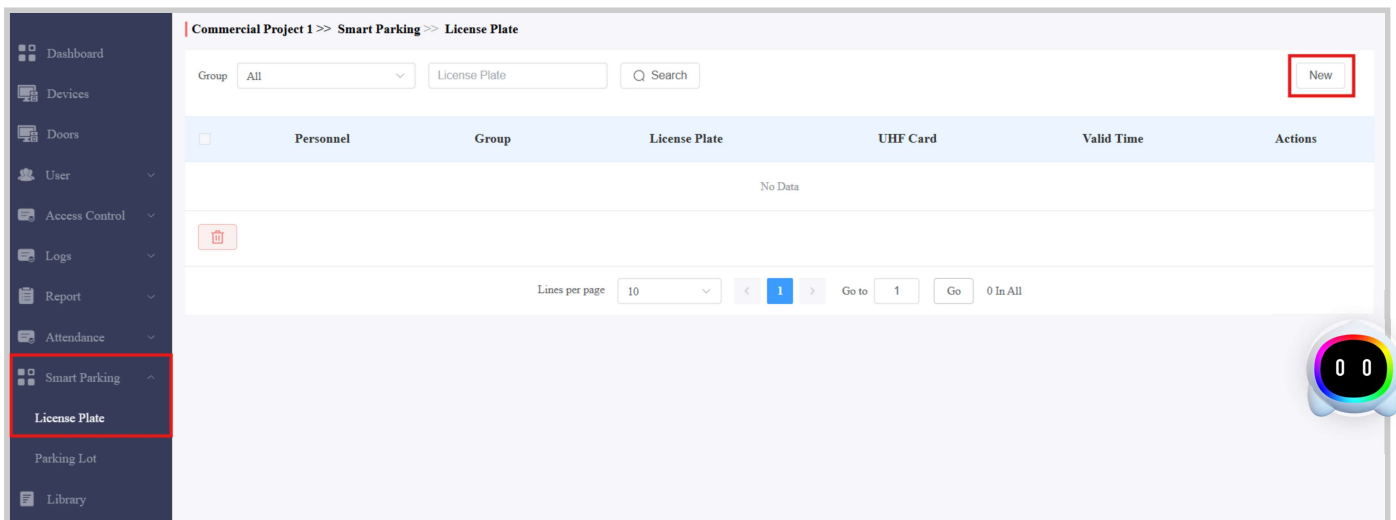
Smart Parking allows you to register license plates or UHF cards for users on the Smart Access Cloud. Users can drive in/out with doors open automatically.

Furthermore, you can manage parking lots by viewing the number of parked vehicles and their parking duration on the cloud, conveniently tracking what happens.

License Plate Management

- The license plates are identified by third-party LPR cameras for door opening. Click [here](#) to view the detailed configuration.
- The UHF cards are identified by the Akuvox long-range access card reader ACR-CRP12 for door opening. Click [here](#) to view the detailed configuration.

1. Click **Smart Parking > License Plate > New**.



2. Select the group and user.

3. Enter the license plate information.

4. Enter the UHF card code if it is used. If you have filled in both the license plate and the UHF card, the cloud will ONLY issue the latter to the door phone.
5. Enable/disable **Set Valid Time**. If enabled, specify when the vehicle can enter or exit the parking lot.

* Group

* License Plate

UHF Card ?

☐ Set Valid Time

Submit

Note

You can also add license plate information when [adding or editing personnel](#).

Parking Lot Management

You can set up parking lots and conveniently track the number of parked vehicles and their parking durations.

Click [here](#) to view the configuration steps.

Dashboard

Devices

Doors

User

Access Control

Logs

Report

Attendance

Smart Parking

License Plate

Parking Lot

Library

Commercial Project 1 >> Smart Parking >> Parking Lot

Name

Search

New

	Name	Parked Vehicles	Door	Actions
	Parking Lot	0	Entry: Front Door - Door1 Exit: Front Door - Door2	? 🗑️

🗑️

Lines per page

10

<

1

>

Go to

1

Go

1 In All

00

Logs

You can check door logs, call history, images captured, alarm logs, and [door opened timeout](#) logs in the **Logs** module.

Door Logs

Door logs have 7 types. You can narrow your log check by the specific time range with parameters: **Device Name**, **Initiated by**, **Action**, **Key**, and **Response**(Success, Failed, or Offline) for the targeted search.

- All: Display all door logs.
- Call: Display the SIP/IP-based calls initiated on the door phone, indicating when, where, and to whom the calls are made.
- Door Release: Display when, where, and by whom the door openings are made (be it failure or success).
- Entry: Display the valid door-opening records of entering without disobeying the [area restriction rules](#).
- Exit: Display the valid door-opening records of the exit without disobeying the area restriction rules.
- Entry Violation: Display the door-opening records of entries that violate the area restriction rules.
- Exit Violation: Display the door-opening records of exits that violate the area restriction rules.



Akuvox

Property Manager Portal

Akuvox Test3 Luna Log out

Installer Portal

Dashboard

Devices

Doors

User

Access Control

Logs

Alarm Records

Attendance

Smart Parking

Library

Akuvox Test3 >> Logs >> Logs

Door Logs

Call History

Capture

Motion Alerts

Operation Logs

Door logs will be kept for 30 days.

Log Type: All

Date: -

Action: All

Device: All

Initiated By:

Response: All

Key:

Search

Happened On	Door	Initiated By	Log Type	Action	Key	Response	Detail	Capture
09-01-2026 06:54:23 AM	Entrance	visitor	Door Release	Face Unlock	--	Failed	--	
07-01-2026 07:26:02 AM	Entrance	visitor	Door Release	Face Unlock	--	Failed	--	
25-12-2025 09:53:01 AM	Entrance	visitor	Door Release	Face Unlock	--	Failed	--	
25-12-2025 09:52:23 AM	Entrance	visitor	Door Release	Face Unlock	--	Failed	--	
25-12-2025 09:43:10 AM	Entrance	visitor	Door Release	Face Unlock	--	Failed	--	

Access Failure Reasons

The cloud provides clear failure reasons when an access attempt is denied under different scenarios.

Failure Scenario	Description	
Invalid credentials	Credentials not registered	E
Holiday restriction	Access attempted during a holiday period	N
No permission / Door inactivated or expired	User has no permission, outside schedule, or door inactivated/expired	N
Vehicle validity expired	License plate is outside the valid period	N
User validity expired	User validity period has expired(applies to PIN, RF card, license plate, face, Bluetooth, NFC, Amenity Reservation, and fingerprint authentication)	C
Door interlock	Access blocked due to door interlock	D
Two-factor authentication failure	Second authentication method does not match configuration	T
Parking limit reached	Parking capacity allocation exceeded	P

You can check the reason in the **Detail** column.

Door Logs will be kept for 30 days.								
Log Type:	All	Date:		-		Action:	All	Device: All
Initiated By:		Key:		Search	Export Logs			
Happened On	Door	Initiated By	Log Type	Action	Key	Response	Detail	Capture
11-12-2025 02:41:29 PM	Entrance-Door1	visitor	Entry	RF Card Unlock	72221021	Failed	Invalid RF Card code	
11-12-2025 11:40:26 AM	Front Door-Door1	Monica Geller	Entry	PIN Unlock	****	Success	---	
11-12-2025 11:40:26 AM	Front Door-Door2	Monica Geller	Exit	PIN Unlock	****	Success	---	
11-12-2025 10:03:13 AM	Front Door	P M	Door Close	Manually Lock	---	Success	---	

Note

Failure reasons may vary depending on device model and firmware version.

Call Logs

You can check when and by whom the SIP calls are made and received. Moreover, you can set the time range or enter the caller or receiver to check the targeted call information.

Commercial Project 1 >> Logs >> Logs			
Door Logs	Call History	Capture	Motion Alerts
Operation Logs			
Call history will be kept for 30 days			
Date:		-	
Caller Or Receiver		Search	Export Logs
Happened On	Caller	Receiver	Call Duration
No Data			
Lines per page 10			
< 1 > Go to 1 Go 0 In All			

Captured Images

Image capturing is either initiated manually by users or by the project manager. You can check when, where, how, and by whom the images are captured. You can click the image in the **Capture** column to see a larger picture.



Commercial Project 1 >> Logs >> Logs				
Door Logs	Call History	Capture	Motion Alerts	Operation Logs
Capture will be kept for 30 days.				
Date:		-		Search
Happened On	Device	Initiated By	Action	Capture
No Data				
Lines per page 10 Go to 1 Go 0 In All				

Motion Alerts

Motion alerts allow you to check the captured image of people whose movement has triggered the motion detection in the door phones (door phones with motion detection function).

Commercial Project 1 >> Logs >> Logs				
Door Logs	Call History	Capture	Motion Alerts	Operation Logs
Motion alerts will be kept for 30 days.				
Date:		-		Search
☐	Happened On	Building	Device	Actions
No Data				
☐				
Lines per page 10 Go to 1 Go 0 In All				

Operation Logs

You can check who has made configurations in the project on the cloud.



Commercial Project 1 >> Logs >> Logs					
Door Logs	Call History	Capture	Motion Alerts	Operation Logs	
Type:	All	Role:	All	Info:	Search by info field
Year:	2025				
Happened On:	- Q Search				
Happened On	Role	Initiated By	Type	Description	Actions
11-10-2025 02:55:55 PM	Property Manager		Personnel	Update: Lyna F	
11-10-2025 02:24:24 PM	Property Manager		Parking Lot	Create: Parking Lot	
11-10-2025 02:24:05 PM	Property Manager		License Plate	Create: UHD223S	
11-10-2025 02:08:33 PM	Property Manager		Muster Report	Update	
11-10-2025 01:55:42 PM	Property Manager		Delivery	Create: Delivery	
11-10-2025 01:48:26 PM	Property Manager		Temp Key	Create: Visitor 1	

Alarm Records

You can check various alarm records on the **Logs > Alarm Records** module.

Emergency Alarm

The emergency alarm is recorded when the [emergency unlock](#) occurs.

Narrow the search by entering a specific time.

Commercial Project 1 >> Logs >> Alarm Records	
Emergency Alarm	Arming Alarm
Door Opened Timeout Alarm	Tamper Alarm
Break-in Alarm	
Alarm Time	- Q Search Export Logs
Alarm Time	Device
No Data	
Lines per page 10 1 Go to 1 Go 0 In All	

Arming Alarms



The alarm is recorded when indoor monitors trigger the arming alarms. Narrow the search by entering a specific time.

Commercial Project 1 >> Logs >> Alarm Records

Emergency Alarm
Arming Alarm
Door Opened Timeout Alarm
Tamper Alarm
Break-in Alarm

Alarm Time
-
Search
Export Logs

Alarm Time	Device	Information
No Data		

Lines per page: 10
1
Go to: 1
Go
0 In All

Door Opened Timeout Logs

When the door-opening time exceeds [a certain limit](#), the alarm will be triggered and recorded.

Commercial Project 1 >> Logs >> Alarm Records

Emergency Alarm
Arming Alarm
Door Opened Timeout Alarm
Tamper Alarm
Break-in Alarm

Alarm Time
-
Search
Export Logs

Alarm Time	Door
No Data	

Lines per page: 10
1
Go to: 1
Go
0 In All

Tamper Alarm

When the device's [tamper alarm](#) is triggered, the alarm will be recorded on the cloud.

Compatible models and versions(or higher):

Model	Version	Model	Version
R20	320.30.11.30	A08	108.30.11.8
R25	25.30.10.117	A01/A02	101.30.10.206
R28	228.30.10.213	A03	103.30.10.204
R29	29.30.10.404	A094	92.30.10.205
X915V2	2915.30.10.420	A095	95.30.10.110

X912	912.30.11.107	E16 V2	216.30.10.208
E12V2	312.30.11.18	S539	539.30.10.507
X916	916.30.10.508	S535	535.30.11.8

Commercial Project 1 >> Logs >> Alarm Records

Emergency Alarm
Arming Alarm
Door Opened Timeout Alarm
Tamper Alarm
Break-in Alarm

Alarm Time
-
Search
Export Logs

Alarm Time	Device Name
No Data	

Lines per page 10
1
Go to 1
Go
0 In All

Break-in Alarm

When someone forcibly opens doors, the [break-in alarm](#) will be triggered and recorded on the cloud.

Commercial Project 1 >> Logs >> Alarm Records

Emergency Alarm
Arming Alarm
Door Opened Timeout Alarm
Tamper Alarm
Break-in Alarm

Alarm Time
-
Search
Export Logs

Alarm Time	Door
No Data	

Lines per page 10
1
Go to 1
Go
0 In All

Event Report

The feature allows for quick data filtering to generate reports, such as personnel entries and exits during a specific time period or alarm events.



Compatible models and versions(or higher):

- X912: 912.30.12.207
- X915V2: 2915.30.10.707
- X916: 916.30.10.508

- R29: 29.30.10.712
- R28V2: 228.30.11.17
- R20: 320.30.12.16
- E16V2: 216.30.11.107
- S539: 539.30.10.605
- S535: 535.30.11.8
- A08: 108.30.11.210
- A01/A02: 101.30.11.109
- A03: 103.30.11.6
- A095: 95.30.11.6
- A094: 92.30.11.106

1. Click **Report > Event Report**.
2. [Optional] Check the desired user and devices.

Commercial Project 1 >> Report >> Event Report

You can use these four filters to filter the event reports you want. When filter isn't required, don't select the filter option. Choose a Saved Template

User Select the user to view events for.

Search

☐ All (0/4)

☐ Project Managers

☐ (Ungrouped)

☐ Default Group

☐ Marketing

☐ Technical

Devices Select the devices to view events for.

Search

☐ All (0/0)

☐ Front Door

3. Specify the time and time order.
4. Check the desired events.
5. Click **Generate Report** in the PDF or XLSX format. Optionally, save the settings as a template for future use.



🕒

Time Duration

Display events that occurred on a specific date or during a period of time.

Time Mode

☒ All The Time
 ☐ Last 8 Hours
 ☐ Last 1 Day
 ☐ Last 7 Days
 ☐ Last 1 Month

☐ Custom

Sort By

Time (Descending) ▾

📅

Event

Select the type of events to display.

Alarm, Hold Open and Lockdown events prior to feature launch will not be displayed.

Door Events

☒ Valid Access Events
☐ Invalid Access Events
☐ Hold Open
☐ Lockdown

Alarm Events

☐ Emergency Alarm
☐ Arming Alarm
☐ Door Opened Timeout Alarm
☐ Tamper Alarm
☐ Break-in Alarm

📄 Save As New Template

Generate Report ▾

6. Check the field(s) to display in the report.

Dashboard

Devices

Doors

User

Access Control

Logs

Report

Muster Report

Event Report

Attendance

Smart Parking

Library

Commercial Project 1 >> Report >> Event Report >>

< Back

Export Report

Happened Time

03-19-2026 10:18:03
 03-19-2026 10:01:17
 01-04-2026 02:28:38
 01-04-2026 02:27:27
 12-25-2025 02:22:05
 12-25-2025 02:22:00
 12-25-2025 02:21:02 PM

Export Report

* Field Chooser

☒ Happened Time
☒ User
☐ Group
☐ Email
☒ Devices
☐ Doors
☒ Information

Cancel

Submit

Information

Door Lockdown Off
 Door Lockdown On
 Door Lockdown Off
 Door Lockdown On
 Door Lockdown On
 Door Lockdown Off
 Door Lockdown On

7. Submit to download the report.



Printed by [REDACTED] at 16:50 on 10/11/2025

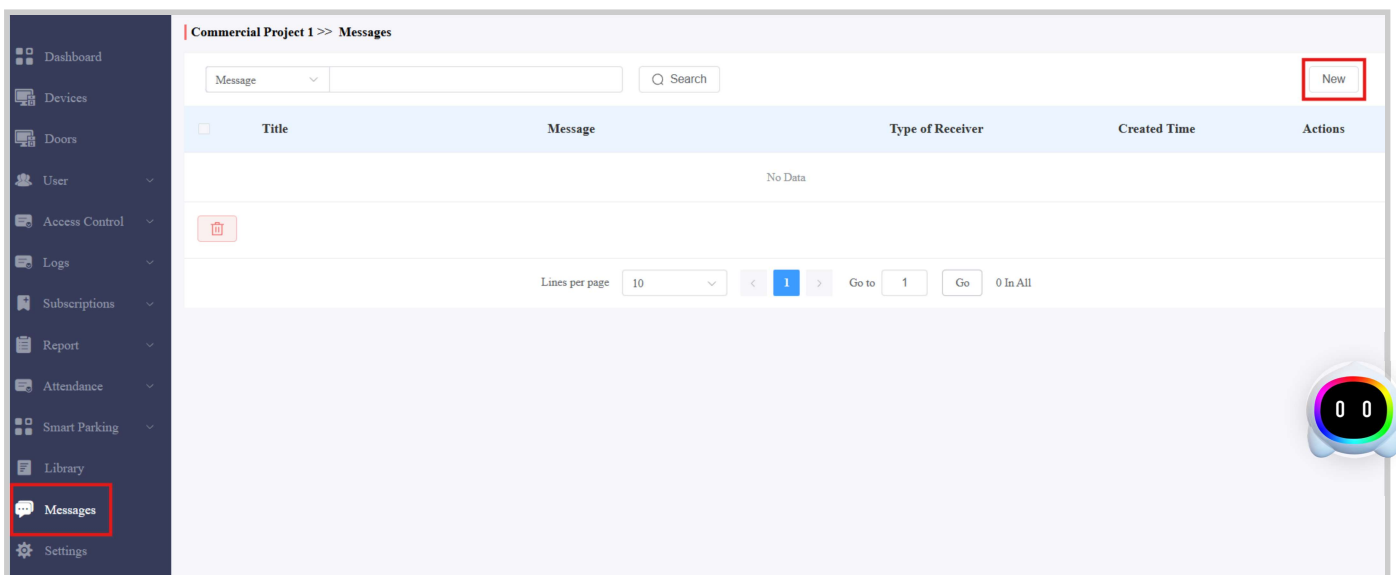
Happened Time	User	Devices	Location	Information
11-10-2025 02:11:45 PM	Lyna F	Front Door	Public Area	Access Granted(PIN Code Unlock)
11-10-2025 02:11:45 PM	Lyna F	Front Door	Public Area	Access Granted(PIN Code Unlock)
11-10-2025 11:38:39 AM	Lyna F	Front Door	Public Area	Access Granted(PIN Code Unlock)
11-10-2025 11:38:39 AM	Lyna F	Front Door	Public Area	Access Granted(PIN Code Unlock)
11-10-2025 10:12:45 AM		Front Door	Public Area	Access Granted(Manually Unlock)
11-07-2025 06:19:40 PM	Rachel Green	Front Door	Public Area	Access Granted(PIN Code Unlock)
11-07-2025 03:38:34 PM	Rachel Green	Front Door	Public Area	Access Granted(PIN Code Unlock)
11-07-2025 03:35:56 PM	Rachel Green	Front Door	Public Area	Access Granted(PIN Code Unlock)
11-07-2025 02:38:47 PM		Front Door	Public Area	Access Granted(Manually Unlock)

Messages

You can create, send, and check messages.

You can create one-time messages or reusable message templates for your convenience.

1. Click **Messages > New**.



2. Enter the message title and content directly to create one-time messages. To create reusable message template(s), click **Add a Template** and enter the

template name, title, and content.

3. Select the receiver type.

+ Add a Template

* Title

* Content

Send To

* Receiver

☐ Indoor Monitor

☒ Personnel App

☒ Admin App

Send

After the message is created, you can click  to check the message details and click  to remove it.

Commercial Project 1 >> Messages

Message

Q Search

Ne

☐	Title	Message	Type of Receiver	Created Time	Actions
☐	Welcome	11	Personnel App, Admin App	11-10-2025 03:27:00 PM	 

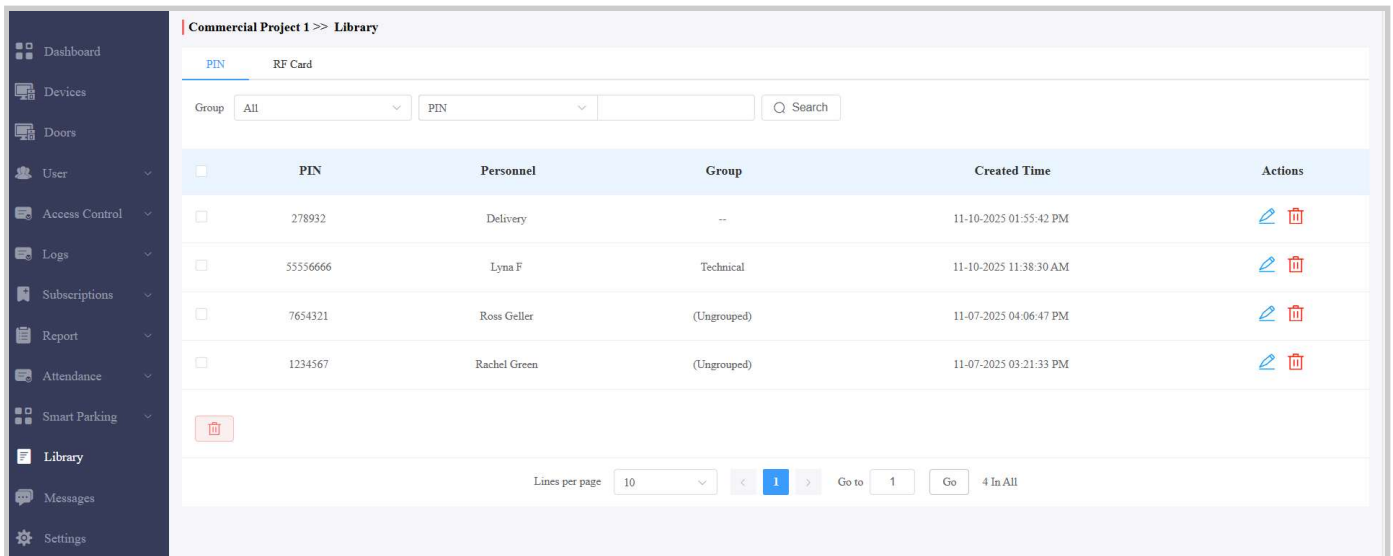


Lines per page 10 < 1 > Go to 1 Go 1 In All

Library

You can check, modify, and delete all types of created PIN codes and RF Cards conveniently at one stop.

On the **Library** module, click  to modify the PIN code or RF card code. Click  to remove the code.



The screenshot shows the 'Library' module interface for 'Commercial Project 1'. It features a sidebar with navigation options: Dashboard, Devices, Doors, User, Access Control, Logs, Subscriptions, Report, Attendance, Smart Parking, Library (selected), Messages, and Settings. The main content area is titled 'Commercial Project 1 >> Library' and has tabs for 'PIN' and 'RF Card'. Below the tabs are filters for 'Group' (set to 'All') and 'PIN' (set to 'PIN'), along with a search bar. A table lists four PIN entries with columns for selection, PIN, Personnel, Group, Created Time, and Actions. The entries are: 278932 (Delivery, --, 11-10-2025 01:55:42 PM), 55556666 (Lyna F, Technical, 11-10-2025 11:38:30 AM), 7654321 (Ross Geller, (Ungrouped), 11-07-2025 04:06:47 PM), and 1234567 (Rachel Green, (Ungrouped), 11-07-2025 03:21:33 PM). Each entry has edit and delete icons in the Actions column. At the bottom, there is a pagination bar showing 'Lines per page' (10), page navigation (1 of 4), and 'Go to' options (1, 4 In All).

	PIN	Personnel	Group	Created Time	Actions
☐	278932	Delivery	--	11-10-2025 01:55:42 PM	 
☐	55556666	Lyna F	Technical	11-10-2025 11:38:30 AM	 
☐	7654321	Ross Geller	(Ungrouped)	11-07-2025 04:06:47 PM	 
☐	1234567	Rachel Green	(Ungrouped)	11-07-2025 03:21:33 PM	 

Settings

Settings include the basic settings(project name, address, permissions, emergency unlock, etc), time settings, and motion detection settings.

Basic Settings

See the description of each item in the chart below.



Dashboard

Devices

Doors

User

Access Control

Logs

Subscriptions

Report

Attendance

Smart Parking

Library

Messages

Settings

Commercial Project 1 >> Settings

Basic Setting

Time Setting

Motion Setting

Emergency Setting

Commercial Name

Commercial Project 1

Commercial Address

Taiwan, China

State/Province

City

Post Code

Street

Allow people to create PIN

☐ On
 ☒ Off

Send email when the device is disconnected.

☐ On
 ☒ Off

Send message when SIM card data exceeds the limit

☐ On
 ☒ Off

Submit

Item Name	Description
Commercial Name	The project name.
Commercial Address	The project address.
Allow people to create PIN.	Set whether users can create PIN codes on th
Send email when the device is disconnected.	Set whether to receive email notifications whe
Send message when SIM card data exceeds the limit.	Set whether to receive email notifications whe LTE function exceed the (SIM card) data pack



Emergency Unlock

You can make all doors open or close automatically or manually during emergencies. For example, in a fire emergency, the doors will automatically open

when an alarm is triggered on any door phone, allowing for quick evacuation. Additionally, all doors can be opened manually.

Note

- With the installer accounts, you can **ONLY** enable/disable the emergency unlock feature but not perform the action.
- With the project manager account, you can click the **Unlock/Lock** button to open or close all doors.
- Click [here](#) to view the models that support this feature and the detailed configuration.

1. Go to **Settings > Emergency Setting**. Select automatic door unlock or manual unlock.
 - Select **On** to open doors automatically when an emergency occurs.
 - Select **Off** to open doors manually on the SmartPlus web portal. You can click **Unlock/Lock** near the top of any interface to open or close the doors manually.
2. Set **Emergency Door Group**. You can select **All Doors** or specific doors to open during an emergency.
3. Set whether to **Unlock All Floors when Emergency Alarm is Triggered**. This option works with Akuvox EC33 elevator control device. When an emergency alarm occurs, all floors controlled by EC33 will be released.
4. Select whether to send notifications to users' SmartPlus Apps and indoor monitors. When enabled, both devices will sound an alert when the emergency unlock happens.



Commercial Project Multi >> Settings

Basic Setting
Time Setting
Motion Setting
Emergency Setting

Unlock Emergency Door Group When Emergency Alarm Triggered

☐ On
☒ Off

Emergency Door Group ?

Unlock All Floors When Emergency Alarm is Triggered

☒ On
☐ Off

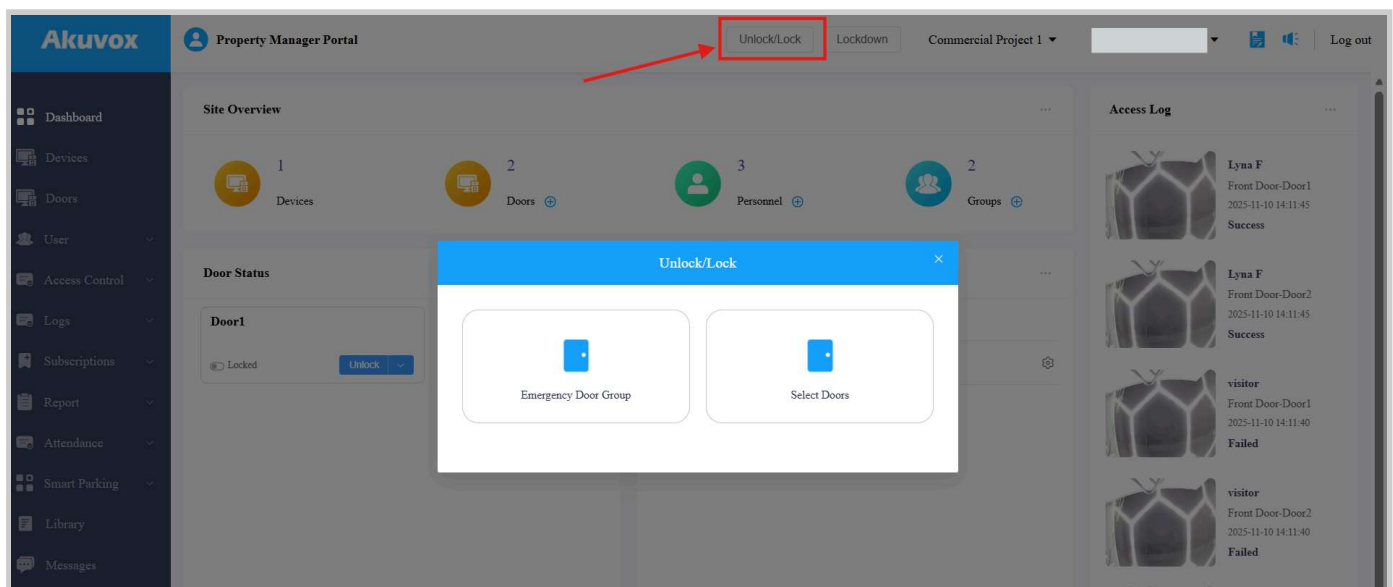
Send Emergency Notifications to Users When Lock/Unlock Emergency Door Group

☐ On
☒ Off

Submit

To open or close doors manually, click **Unlock/Lock**.

- **Emergency Door Group:** Open/close doors you select in the emergency door group.
- **Select Doors:** Open/close specific doors.



Time Settings



You configure and modify the time setting based on the site's location and time zone.

Go to **Settings > Time Settings**.

Commercial Project 1 >> Settings

Basic Setting

Time Setting

Motion Setting

Emergency Setting

Time Zone

UTC+8:00 Shanghai

Time Format

☐ 24-hour time

☒ 12-hour time

Date Format

Month-Day-Year

Submit

Motion Detection

You can enable/disable motion detection, but also set up the device's motion detection type and alert trigger delay.

1. Go to **Settings > Motion Setting**.
2. Set the motion detection:
 - **Disable:** Turn off the function.
 - **IR Detection:** When the infrared sensor detects moving objects, alerts will be triggered.
 - **Video Detection:** When the video camera detects moving objects, alerts will be triggered.
3. Set the **Alert Delay Time** from 5 to 60 seconds.



Commercial Project 1 >>> Settings

Basic Setting

Time Setting

Motion Setting

Emergency Setting

Motion Detection

IR Detection

Alert Delay Time

5s

Submit

Privacy Policy

You will see the **Privacy Policy** and **Terms of Service** window when you log into the platform for the first time.

- The Privacy Policy tells you how the user data is collected, used, and protected.
- The Terms of Service outline the rules and guidelines for using the SmartPlus service.

Only when you click **Agree** can you log into the SmartPlus platform.

Privacy Policy

Privacy Policy

Last updated: October 21st, 2024

Overview of Privacy Policy

Welcome to our service, the service is provided and controlled by SMART-PLUS PTE. LTD. (hereinafter referred to as 'SMART-PLUS', 'us' or 'we'). By using the service, you agree to this Privacy Policy.

The service includes:

- Our website and user accounts that may be accessed at *cloud.akuvox.com, *cloud.akubela.com (*cloud include ecloud, ucloud, jcloud, scloud and so on), and all associated sites connected with it, excluding any third parties' sites (the 'Portal');
- Online services accessible through the Website ('Web Services');
- Software applications that can be downloaded to a mobile device ('Mobile Apps'), such as Akuvox SmartPlus, BelaHome, and so on;
- Related products ('Devices') of the service, including, but not limited to, door phones, indoor monitors, android video phones, access control terminals, and home control panels;
- Any services available on the Website and the Mobile Apps ('Available Services');
- The term 'SERVICE' means the Website, Web Services, Mobile Apps, Devices and Available Services.

The privacy policy describes who we are, what information we collect about you, how we use and disclose your personal information, the details of how we protect your information, and your data privacy rights. Our SERVICE takes your personal information very seriously and gives you control over your personal information. We use robust encryption technology to protect your personal data and privacy, and employ strict policies to manage all data. We will always protect personal data concerning you in accordance with the so-called General Data Protection Regulation ("GDPR") and California Consumer Privacy Act ("CCPA").

A. Who we are

The SERVICE is provided and controlled by SMART-PLUS PTE. LTD. a.s. with the Tax Id. No 202116626G and the registered office in 6 RAFFLES QUAY #14-06, Singapore (048580).

B. What Personal Information We Collect

Personal information is collected by our SERVICE for the purpose of providing services under applicable laws.

"Personal information" shall have the same meaning as "personal data" and shall include any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

We will ask you to provide personal information that is necessary to provide the SERVICE to you. If you do not provide us with any or all of these information, we will not process them, however, the SERVICE or some of its function might be limited.

Disagree

Agree

You can also click **User Agreement** on the left column to check the agreements again.

Dashboard

Company

Personnel

Visitor

Access Control

Logs

Admin

Library

Messages

Devices

Settings

User Agreement

Privacy Policy

Terms of Service

Test2 >> User Agreement >> Privacy Policy

Privacy Policy

Last updated: October 21st, 2024

Overview of Privacy Policy

Welcome to our service, the service is provided and controlled by SMART-PLUS PTE. LTD. (hereinafter referred to as 'SMART-PLUS', 'us' or 'we'). By using the service, you agree to this Privacy Policy.

The service includes:

- Our website and user accounts that may be accessed at *cloud.akuvox.com, *cloud.akubela.com (*cloud include ecloud, ucloud, jcloud, scloud and so on), and all associated sites connected with it, excluding any third parties' sites (the 'Portal');
- Online services accessible through the Website ('Web Services');
- Software applications that can be downloaded to a mobile device ('Mobile Apps'), such as Akuvox SmartPlus, BelaHome, and so on;
- Related products ('Devices') of the service, including, but not limited to, door phones, indoor monitors, android video phones, access control terminals, and home control panels;
- Any services available on the Website and the Mobile Apps ('Available Services');
- The term 'SERVICE' means the Website, Web Services, Mobile Apps, Devices and Available Services.

The privacy policy describes who we are, what information we collect about you, how we use and disclose your personal information, the details of how we protect your information, and your data privacy rights. Our SERVICE takes your personal information very seriously and gives you control over your personal information. We use robust encryption technology to protect your personal data and privacy, and employ strict policies to manage all data. We will always protect personal data concerning you in accordance with the so-called General Data Protection Regulation ("GDPR") and California Consumer Privacy Act ("CCPA").

A. Who we are

The SERVICE is provided and controlled by SMART-PLUS PTE. LTD. a.s. with the Tax Id. No 202116626G and the registered office in 6 RAFFLES QUAY #14-06, Singapore (048580).

B. What Personal Information We Collect

Personal information is collected by our SERVICE for the purpose of providing services under applicable laws.

"Personal information" shall have the same meaning as "personal data" and shall include any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

We will ask you to provide personal information that is necessary to provide the SERVICE to you. If you do not provide us with any or all of these information, we will not process them, however, the SERVICE or some of its function might be limited.

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.

