About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM

S539
DOOR PHONE
Admin Guide

Thank you for choosing the Akuvox S539 series door phone. This manual is intended for administrators who need to properly configure the door phone. This manual applies to version 539.30.10.6, and it provides all the configurations for the functions and features of the S539 series door phone. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

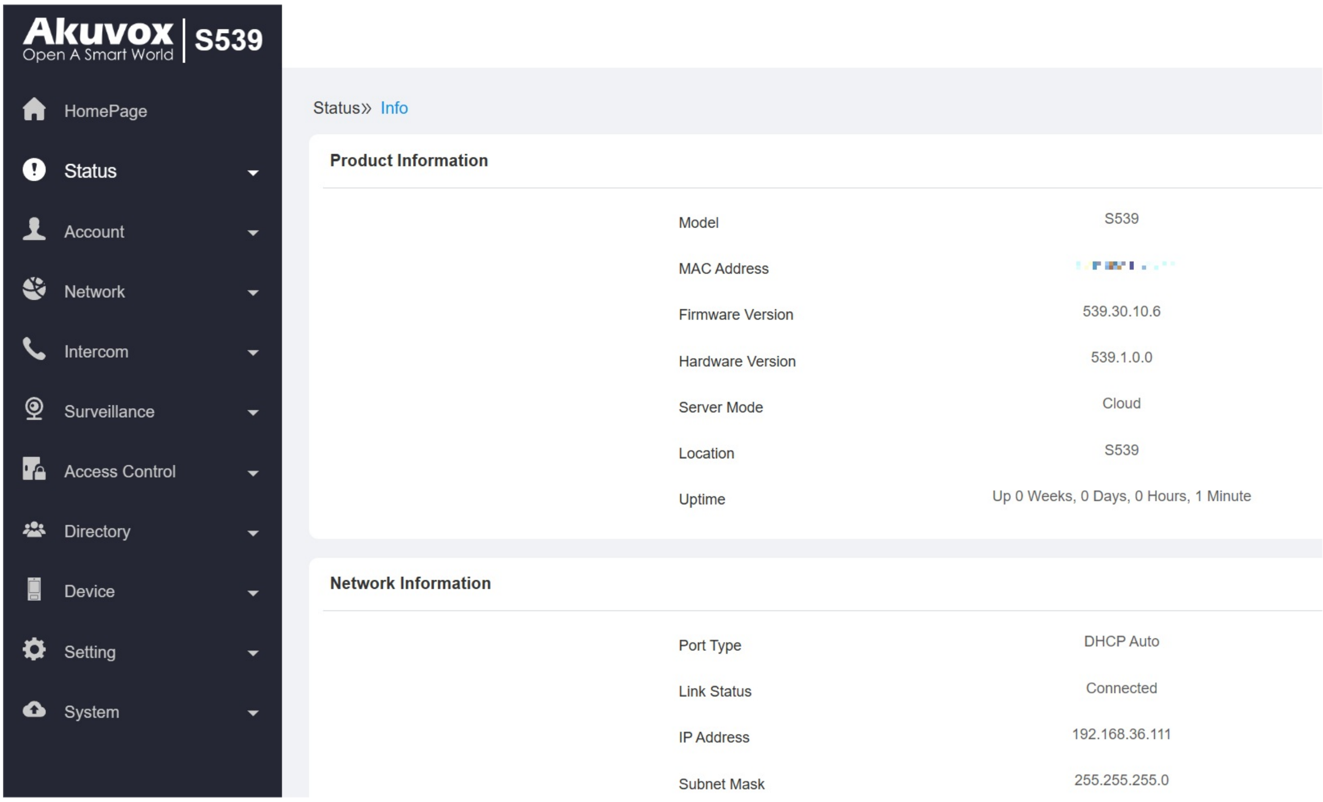
Akuvox S539 series products are Android-based IP video door phones with touch screens. It incorporates audio and video communications, access control, and video surveillance. Its finely tuned Android OS, Cloud, and AI-based communication technology allow featured customization to better suit your operation habit. S539 series multiple ports, such as RS485 and Wiegand ports, can be used to easily integrate external digital systems, such as elevator controllers and fire alarm detectors, helping to create a holistic control of the building entrance and its surroundings and giving you a great sense of security via a variety of access such as card access, NFC, Bluetooth, QR code and newly added voice control door access in an accompaniment with body temperature measurement. S539 series door phones are applicable to residential buildings, office buildings, and their complex.

Model Specification

Model	S539
Touch Screen	✔
Relay In	3
Relay Out	3
Alarm In	X
RS485	✔
Card Reader	13.56MHZ & 125KHZ
Wi-Fi	X
Bluetooth	✔
Temperature Detection	Optional
Face Recognition	✔
LTE	X
USB	X
External SD Card	X

Introduction to Configuration Menu

- **Status**: this section gives you basic information such as product information, network information, call log, and door log,
- **Account**: this section concerns the SIP account, SIP server, proxy server, transport protocol type, audio&video codec, DTMF, session timer, et
- **Network**: this section mainly deals with DHCP&Static IP setting, RTP port setting, device deployment, etc.
- **Intercom**: this section covers intercom settings, call features, dial plans, etc.
- **Surveillance**: this section covers motion detection, RTSP, MJPEG, ONVIF, live stream, etc.
- **Access Control**: this section covers input control, relay, card settings, face recognition settings, Private PIN codes, etc.
- **Directory**: this section involves user management, RF card, PIN, face recognition management, and contact management.
- **Device**: this section includes light settings, LCD settings, audio settings, lift control, Wiegand.
- **Setting**: this section includes time, language, action settings, schedule for access control, screen display, and HTTP API.
- **System**: this section covers firmware upgrade, device reset&reboot, configuration file auto-provisioning, fault diagnosis, security, PCAP, system log, web call, tamper alarm, and password modification.



Product Information

Model S539

MAC Address [redacted]

Firmware Version 539.30.10.6

Hardware Version 539.1.0.0

Server Mode Cloud

Location S539

Uptime Up 0 Weeks, 0 Days, 0 Hours, 1 Minute

Network Information

Port Type DHCP Auto

Link Status Connected

IP Address 192.168.36.111

Subnet Mask 255.255.255.0

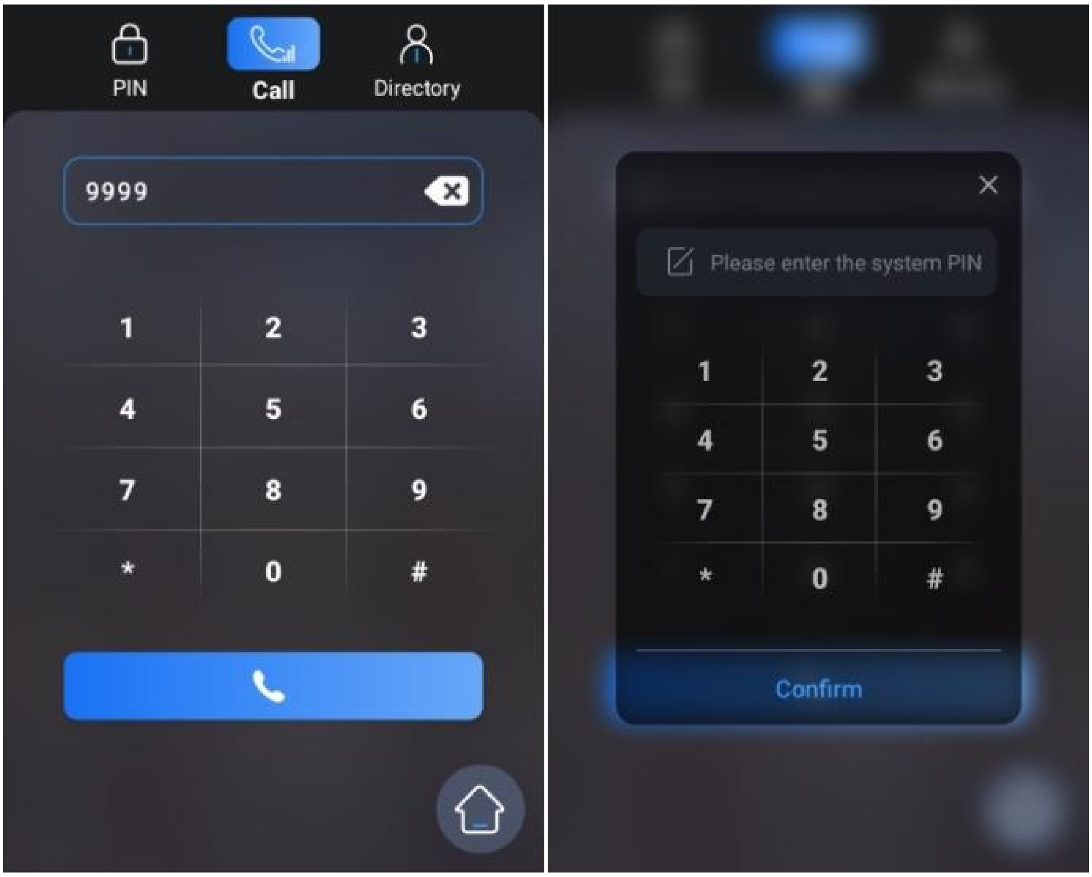
Access the Device

Door phones' system settings can be either accessed on the device directly or on the device web interface.

Access the Device Setting on the Device

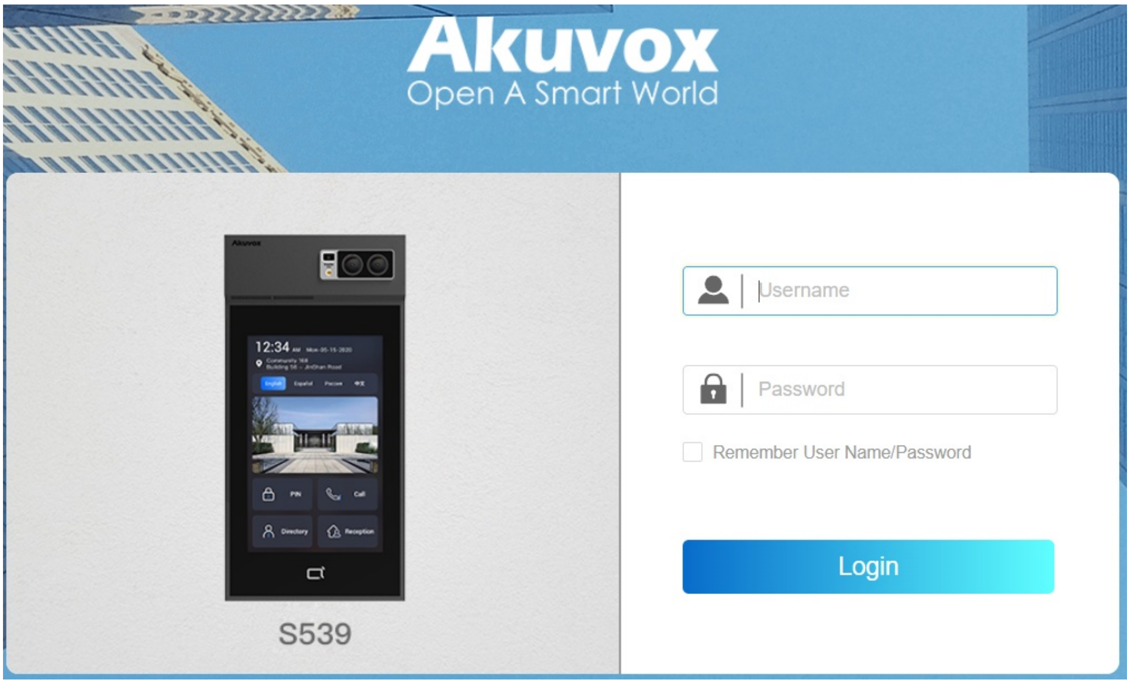
Before configuring door phone, please make sure the device is installed correctly and connected to a normal network.

You can set up some basic settings on the device screen by pressing **9999** + **Dial key** + **3888** (password) on the **Dial** screen.



Access the Device Setting on the Web Interface

You can also enter the device IP address on the web browser in order to log in to the device web interface where you can configure and adjust parameters, etc.



Note

- You can obtain the device IP address using the Akuvox IP scanner to log in to the device web interface.
- To download: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- Detailed guide: https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner
- Google Chrome browser is strongly recommended.
- The initial username and password are **admin** and please be case-sensitive to the user names and passwords entered.

Language and Time Setting

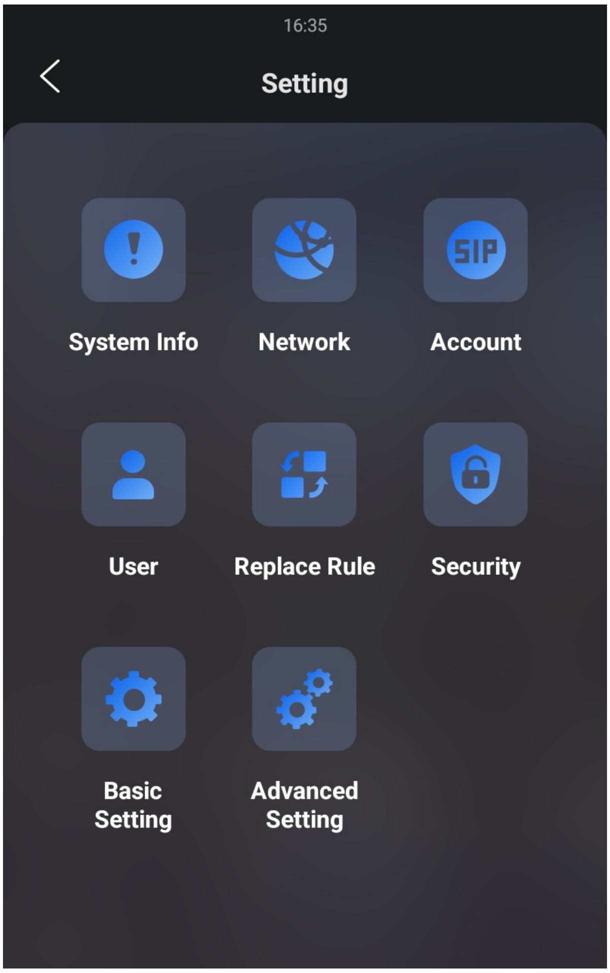
Language Setting

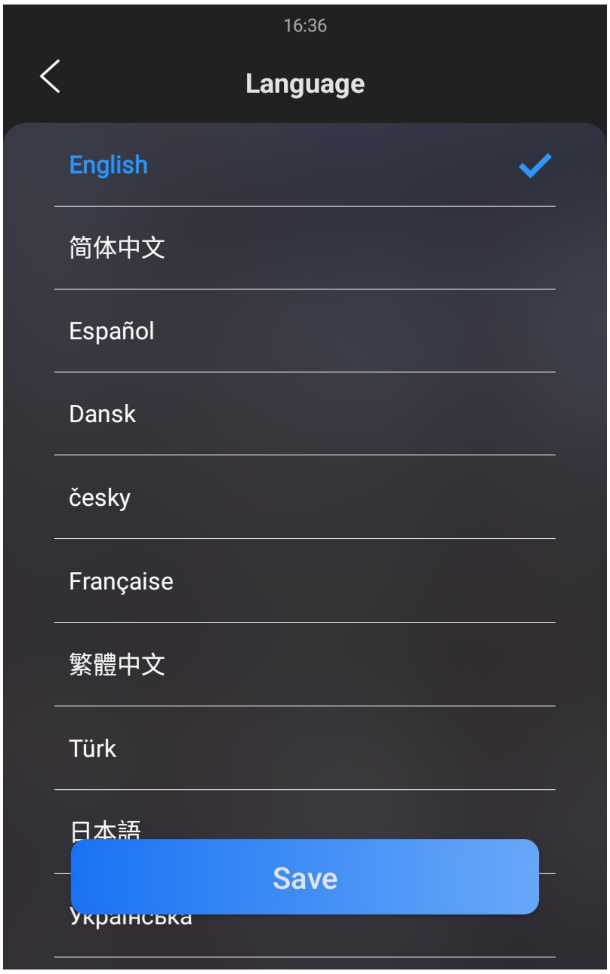
Set up the language during initial device setup or later through the device or web interface according to your preference.

Language Setting on the Device

To configure the language display on the device **Basic Setting > Language** interface.
The device supports the following language:

- Simplified Chinese, English, Spanish, Danish, Czech, French, Traditional Chinese, Turkish, German, Japanese, Ukrainian, Korean, Norsk, Dutch, and Russian.

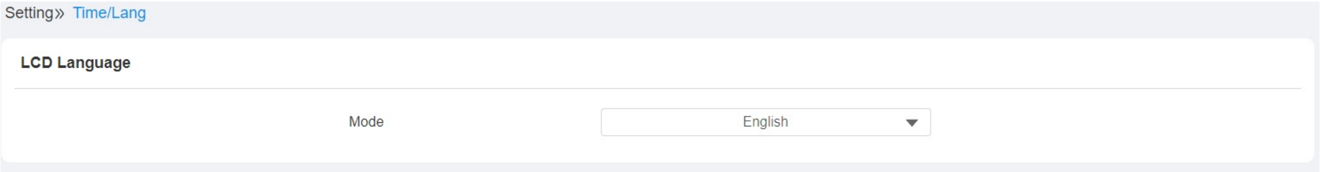




Language Setting on the Device Web Interface

You can select device language and device language icons, and customize interface text including configuration names and prompt text.

To select the device language, go to **Setting > Time/Lang > LCD Language** interface.

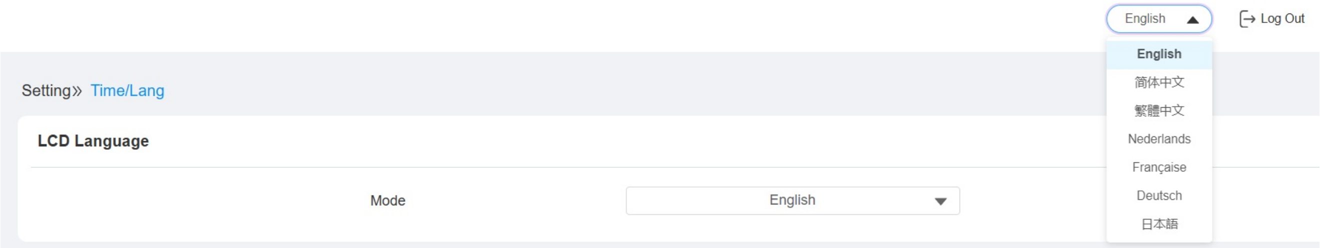


Setting» Time/Lang

LCD Language

Mode: English

You can choose the web language on the upper right corner.

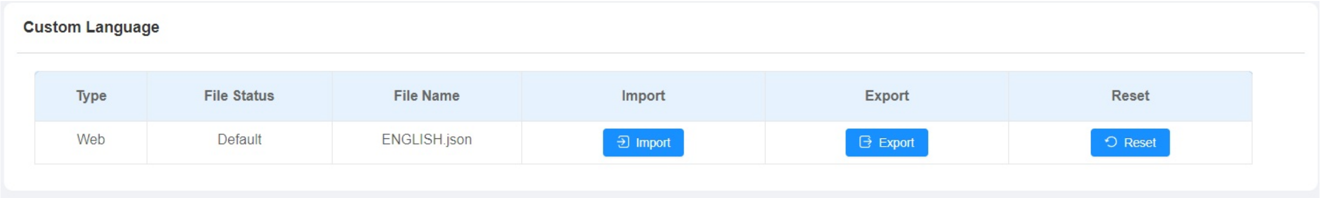


Setting» Time/Lang

LCD Language

Mode: English

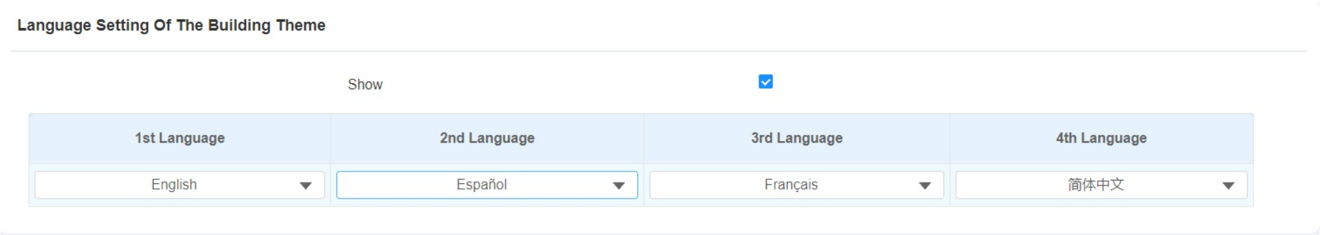
To customize language, you need to export and edit the .json file before uploading the file to the device. Path: **Setting > Time/Lang**.



Custom Language

Type	File Status	File Name	Import	Export	Reset
Web	Default	ENGLISH.json	Import	Export	Reset

To create the language icons for the building mode, go to **Setting > Key/Display > Language Setting Of The Building Theme**.



Language Setting Of The Building Theme

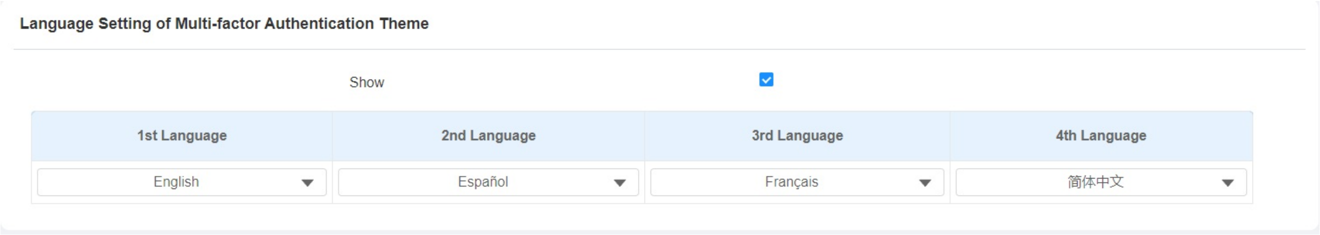
Show ☑

1st Language	2nd Language	3rd Language	4th Language
English	Español	Français	简体中文

Note

- You need to select the building mode or multi-factor authentication mode first before you can set the language icon on the home screen for them.

To create the language icons for the multi-factor authentication mode, go to **Setting > Key/ Display > Language Setting of Multi-factor Authentication Theme**.



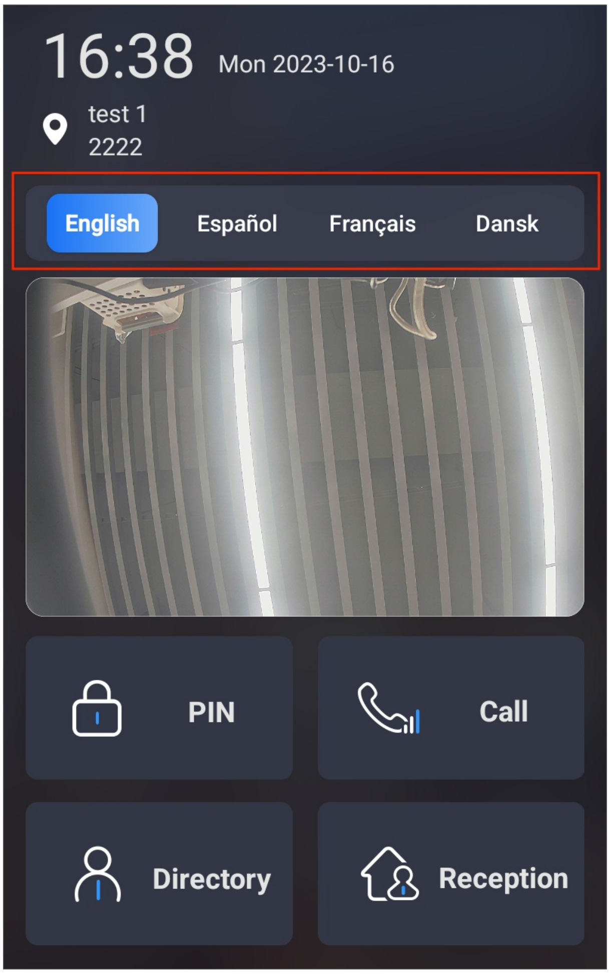
Language Setting of Multi-factor Authentication Theme

Show ☑

1st Language	2nd Language	3rd Language	4th Language
English	Español	Français	简体中文

Parameter Set-up:

- **Visible**: enable it if you want the four language icons to be displayed on the home screen for the language selection.
- **Language 1/2/3/4**: select the order that the language display. For example, if you set the 1st language as English, then the English language will be displayed first from left to right on the screen.

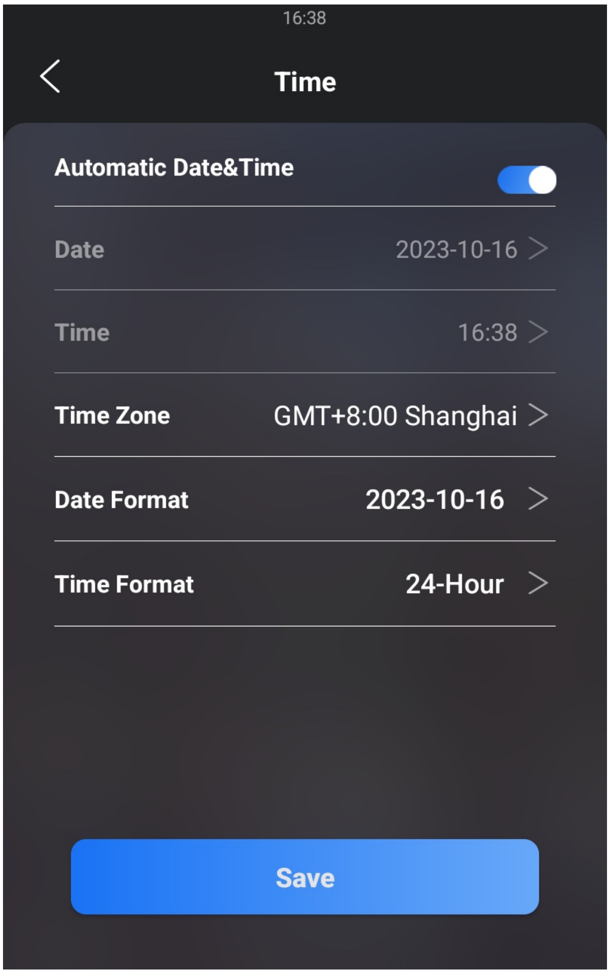


Time Setting

Time settings, including time zone, date and time format, and more, can be configured either on the device or the web interface.

Time Setting on the Device

To configure the language display on the device **Basic Setting > Time** interface.



16:38

Time

Automatic Date&Time

Date 2023-10-16

Time 16:38

Time Zone GMT+8:00 Shanghai

Date Format 2023-10-16

Time Format 24-Hour

Parameter Set-up:

- **Automatic Date&Time:** Automatic Date is toggled on by default, which allows the date& time to be automatically set up and synchronized with the default time zone and the NTP server (**Network Time Protocol**). You can also set it up manually by toggling off the switch first and then entering the time and date you want before pressing the Save tab for the validation.

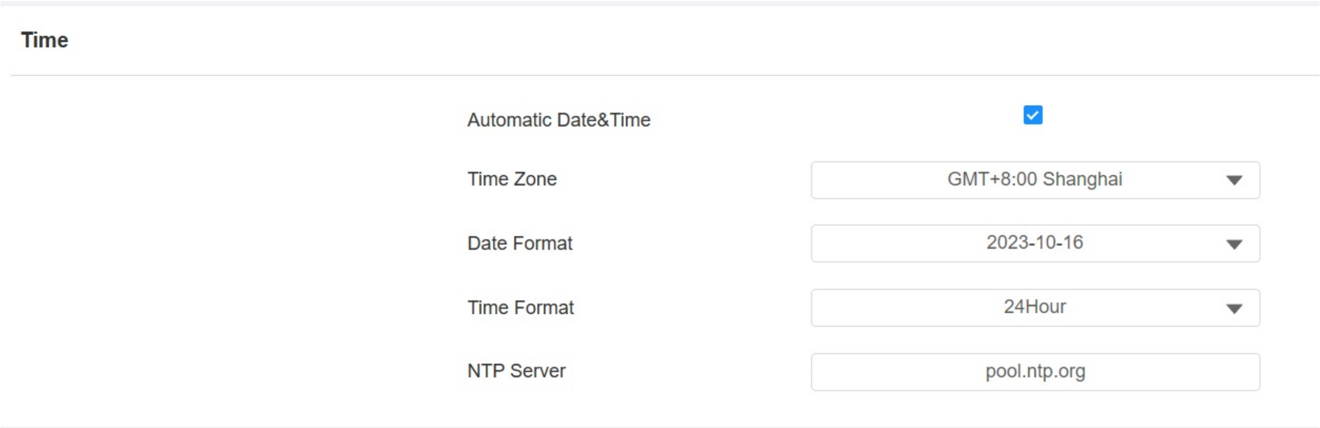
Note

- When the **Automatic Date&Time** toggle switch is toggled off, parameters related to the NTP server will become not editable. And when the switch is toggled on, time and date will be denied editing.

Time Setting on the Device Web Interface

Time settings on the web interface allows you to set up the NTP server address that you obtained to automatically synchronize your time and date. When a time zone is selected, the device will automatically notify the NTP server of the time zone so that the NTP server can synchronize the time zone setting in your device.

To configure the configuration on the web **Setting >Time/Lang > Time** interface.



Time

Automatic Date&Time	☑
Time Zone	GMT+8:00 Shanghai
Date Format	2023-10-16
Time Format	24Hour
NTP Server	pool.ntp.org

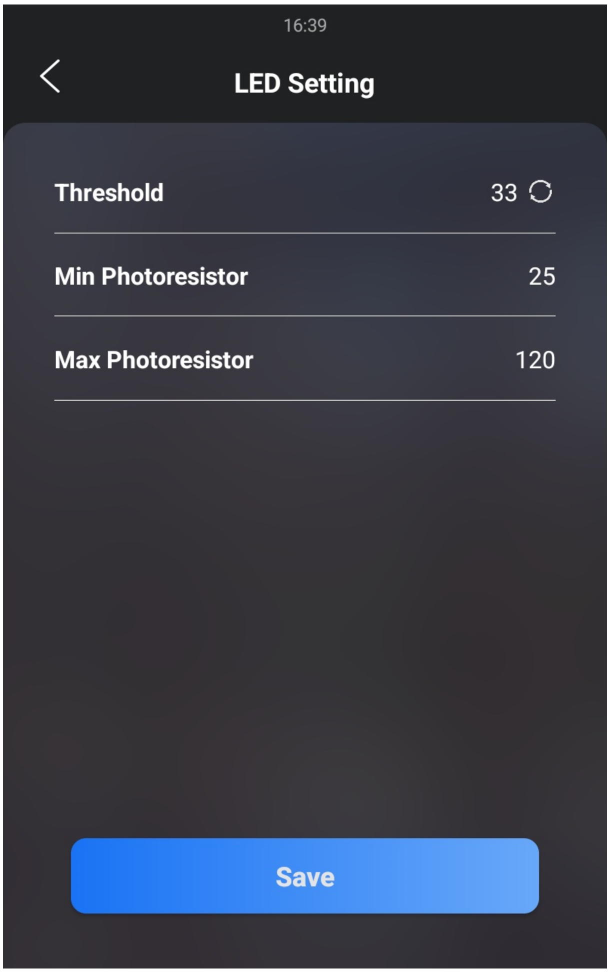
LED&LCD Setting

Infrared LED Setting

Infrared LED is mainly designed to reinforce the light for facial recognition at night or in a dark environment, you can configure the infrared LED in the device and on the web interface.

Infrared LED Setting on the Device

To configure it on the device **Basic Setting > Display > LED Setting** interface.



16:39

LED Setting

Threshold 33

Min Photoresistor 25

Max Photoresistor 120

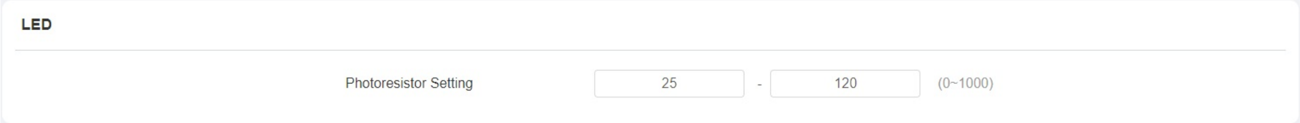
Parameter Set-up:

- **Threshold**: refers to the current light intensity indicated by the photo-resistor value. The higher photo-resistor values correspond conversely to the lower light intensity and vice versa. The default photo-resistor value (**Threshold**) is 33, however, you can tap the icon ⟳ several times in order to obtain the actual photo-resistor value in a specific environment (the value fluctuation is about 5), and the value is what you based on configure the minimum and maximum photo-resistor values.

- **Min/Max Photoresistor**: set the minimum and maximum photoresistor value based on the current actual photo-resistor value detected to control the **ON-OFF** of the LED light. You can set the maximum photoresistor value for the IR LED to be turned on and the minimum value for it to be turned off. While the default minimum and maximum photoresistor values are from **0** minimum to **1000** maximum.

Infrared LED Setting on the Web Interface

To configure the configuration on the web **Device** > **Light** > **LED** interface.



LED

Photoresistor Setting 25 - 120 (0~1000)

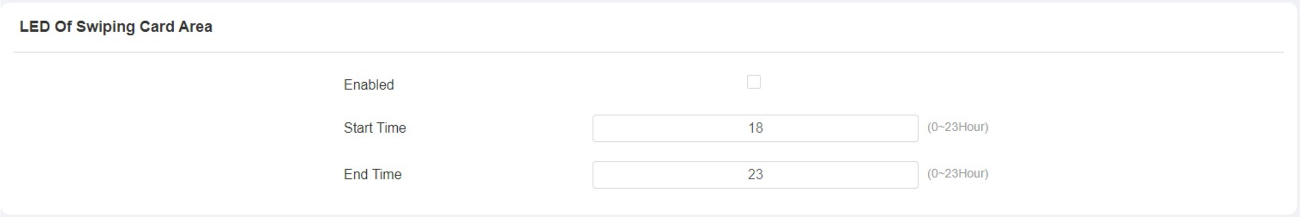
Note

- Please refer to the infrared LED parameter setting on the device.

LED Setting on Card Reader Area

You can enable or disable the LED lighting on the card reader area as needed on the web interface. Meanwhile, if you do not want to have the LED light on the card reader area stay on, you can also set the timing for the exact time span during which the LED light can be disabled in order to reduce electrical power consumption.

To configure the configuration on the web **Device** > **Light** > **LED Of Swiping Card Area** interface.



LED Of Swiping Card Area

Enabled □

Start Time 18 (0~23Hour)

End Time 23 (0~23Hour)

Parameter Set-up:

- **Start Time- End Time(H)**: enter the time span for the LED lighting to be valid, eg., if the time span is set from **8-0 (Start time- End time)**, it means the LED light will stay on during the time span from **8:00** am to **12:00** pm during one day (24 hours).

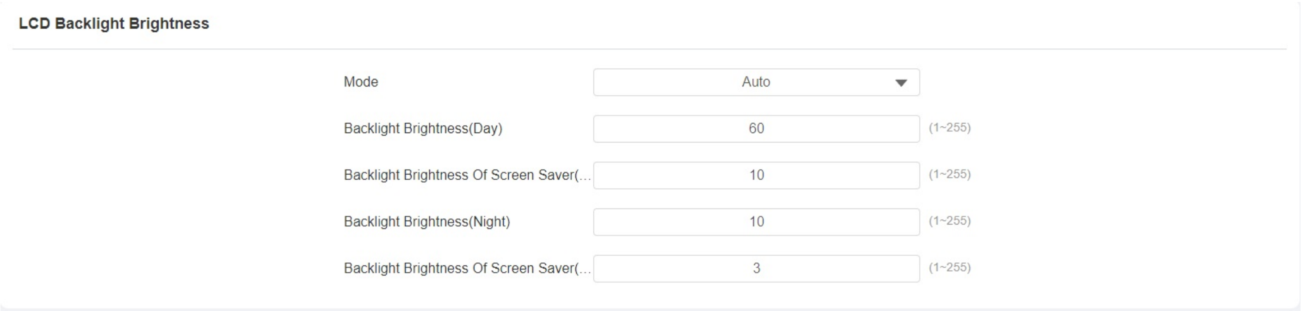
LCD Screen Brightness Setting

If you want to brighten up the screen in order to see the screen at greater ease in an environment with higher light intensity, you need to set up the related parameters.

LCD Screen Brightness Setting on the Web Interface

On the web interface, you can set and adjust the backlight brightness for the screen and screen saver.

To configure the configuration on the web **Device** > **Light** > **LCD Backlight Brightness** interface.



LCD Backlight Brightness

Mode	Auto	
Backlight Brightness(Day)	60	(1~255)
Backlight Brightness Of Screen Saver(...	10	(1~255)
Backlight Brightness(Night)	10	(1~255)
Backlight Brightness Of Screen Saver(...	3	(1~255)

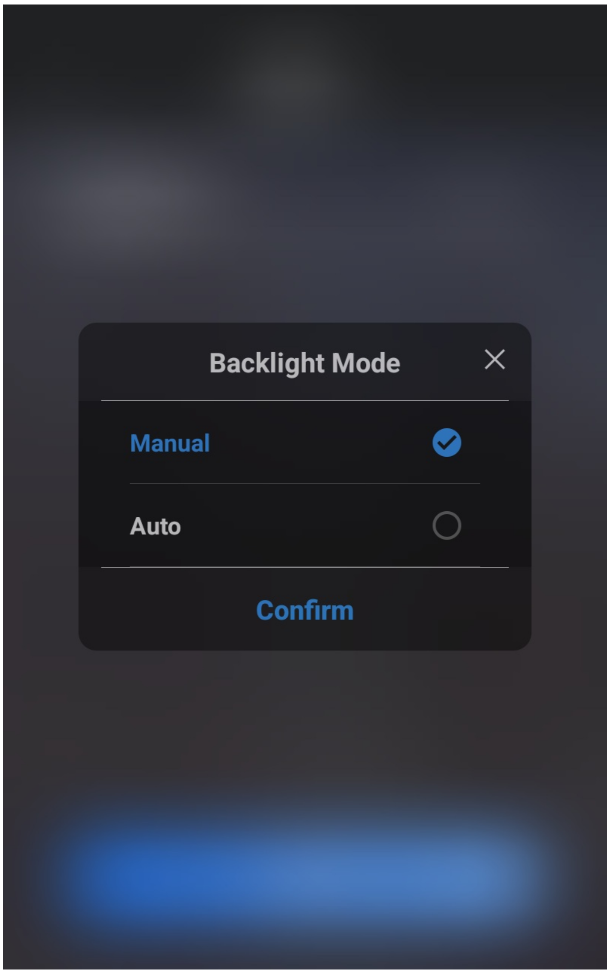
Parameter Set-up:

- **Mode**: click to select **Manual** or **Auto** mode for the backlight. The backlight will be adjusted automatically for the screen backlight brightness when **Auto** is selected and vice versa.
- **Backlight Brightness (day)**: set the screen backlight brightness during the daytime with the value ranging from (**0-255**).
- **Backlight Brightness Of Screen Saver(day)**: set the screen backlight brightness for the screen saver during the daytime with the value ranging from (**0-255**).
- **Backlight Brightness(night)**: set the screen backlight brightness at night with the value ranging from (**0-255**).
- **Backlight Brightness Of Screen Saver(night)**: set the screen backlight brightness for the screen saver during the daytime with the value ranging from (**0-255**).

LCD Screen Brightness Setting on the Device

On the device, you can set and adjust the screen backlight brightness.

To configure it on the device **Basic Setting** > **Display** > **LCD Setting** interface.

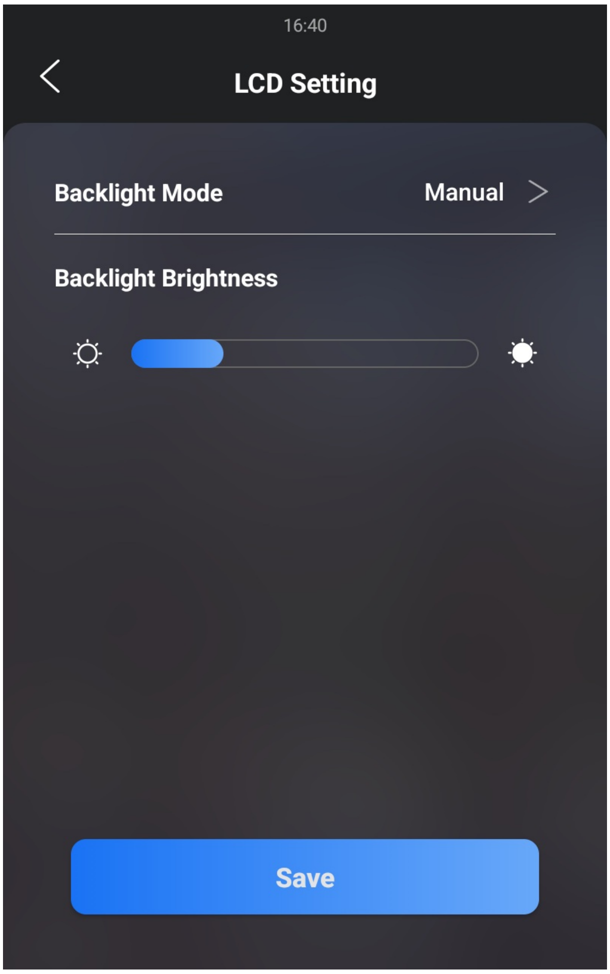


Backlight Mode ✕

Manual ✓

Auto ○

Confirm



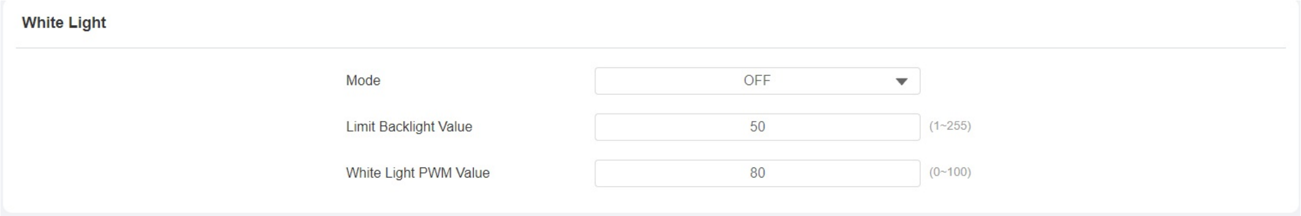
Backlight Mode: Manual

Backlight Brightness

LED White Light Setting

White light LED is mainly used to reinforce the lighting for the QR code access and for the greater visibility of the visitors when seeing their images from indoors in a dark environment.

To configure it on the web **Device > Light > White Light** interface.



White Light

Mode	OFF	
Limit Backlight Value	50	(1~255)
White Light PWM Value	80	(0~100)

Parameter Set-up:

- **Mode**: select **Auto** or **OFF**. If you select **Auto**, the white light will turn on for 5 minutes for facial recognition and QR code scan.

Screen Display Configuration

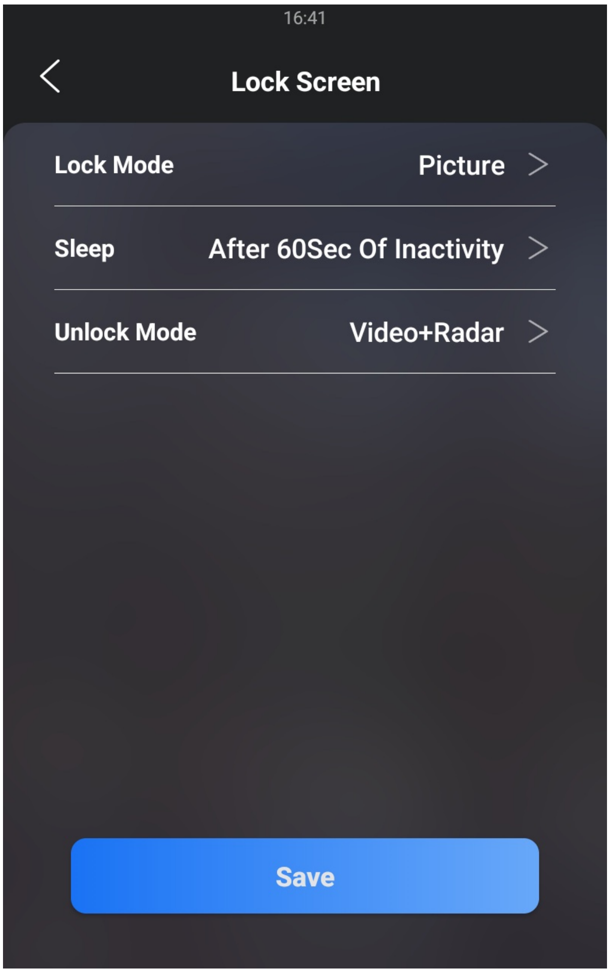
You can set up the device's screen display features such as screensaver to give users a better visual and operational experience.

Screensaver Configuration

Configure Screensaver on the Device

Sleep mode and screen saver are designed for screen protection. You can set these two modes to prevent the device screen from getting overheated and to reduce energy consumption. You can define when the device should go into sleep mode, screen saver mode, and turn off the screen.

On the device screen, go to **Basic Setting > Lock Screen.**



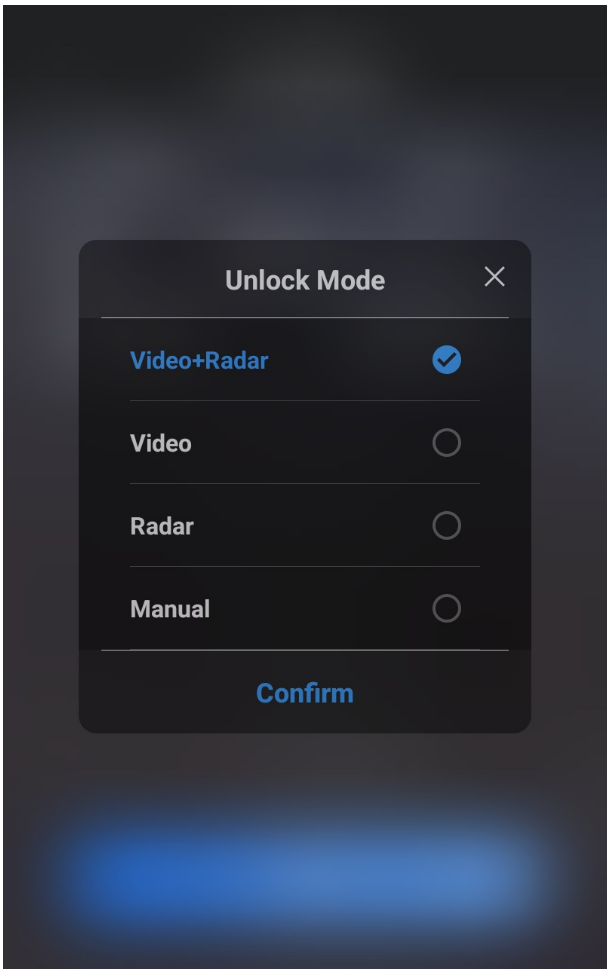
16:41

Lock Screen

Lock Mode: Picture

Sleep: After 60Sec Of Inactivity

Unlock Mode: Video+Radar



Unlock Mode

Video+Radar ☑

Video ○

Radar ○

Manual ○

Parameter Set-up:

- **Lock Mode**: select among three options **NONE**, **Blank Screen**, and **Picture. NONE** is selected when you want the screen to stay on without going into screen saver mode; if **Blank Screen** is selected, the screen will go black. If **Picture** is selected, then the picture you uploaded will be shown as the screen saver.

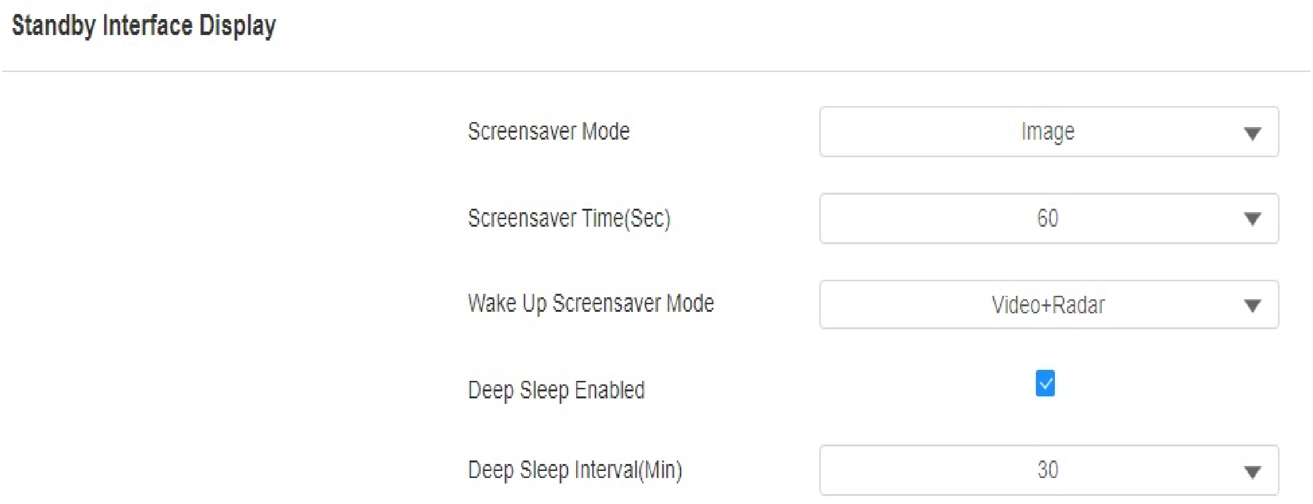
- **Sleep**: set the screen saver start time from 5 seconds up to 180 seconds. The screen saver starts when the device detects no operation, or no one is approaching.

- **Unlock Mode**:
  a. select **Manual**, if you want to wake up the screen manually by tapping the touch screen.
  b. select **Video**, the device screen will be wakened up when an object is detected in the video image.
  c. Select **Radar**, then the device screen will be wakened up when an object is detected by the Radar.
  d. Select **Radar+Video**, then the device will be wakened up when an object is detected by Radar or video image.

Configure Screensaver on the Web Interface

You can set the screen saver duration as well as the timing for the screen to be turned off for both screen protection and power reduction.

To configure the configuration on the web **Device** > **LCD** > **Standby Interface Display** interface.



Standby Interface Display

Screensaver Mode: Image

Screensaver Time(Sec): 60

Wake Up Screensaver Mode: Video+Radar

Deep Sleep Enabled: ☑

Deep Sleep Interval(Min): 30

Parameter Set-up:

- **Screensaver Mode**: select among three options **NONE**, **Blank**, and **Image**. **NONE** is selected when you want the screen to stay on without going into screen saver mode; if **Blank** is selected, the screen will go black. If **Image** is selected, then the picture you uploaded will be shown as the screen saver.

- **Screensaver Time (Sec)**: set the screen saver start time from 5 seconds up to 180 seconds. The screen saver starts when the device detects no operation, or no one is approaching.

- **Wake Up Screensaver Mode**: select the screen wake-up mode.
  a. select Manual, if you want to wake up the screen manually by tapping the touch screen.
  b. select Video, the device screen will be wakened up when an object is detected in the video image.
  c. select Radar, then the device screen will be wakened up when an object is detected by the Radar.
  d. select Radar+Video, then the device will be wakened up when an object is detected by Radar or video image.

- **Deep Sleep Enabled**: tick the check box if you want the screen to be turned off after the screensaver reaches the end of duration as predefined.
- **Deep Sleep Interval (Min)**: set the screensaver time duration before the screen can be turned off.

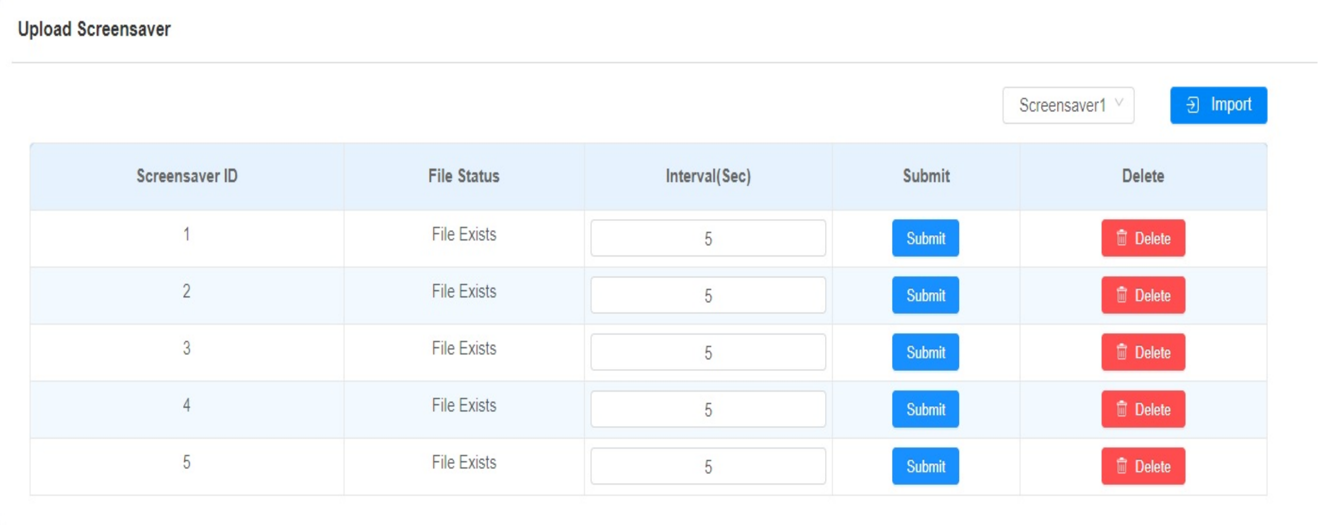
Note

- **Wake Up Screensaver Mode** cannot be changed from **Auto** to **Manual** when the **Screensaver Mode** is set as **Blank Screen.**

Upload Screensaver

You can upload screen-saver pictures separately or in batches to the device and to the device web interface for publicity purposes or for a greater visual experience.

To configure the configuration on the web **Device > LCD > Upload ScreenSaver** interface.



Upload Screensaver

Screensaver1 ∨ Import

Screensaver ID	File Status	Interval(Sec)	Submit	Delete
1	File Exists	5	Submit	Delete
2	File Exists	5	Submit	Delete
3	File Exists	5	Submit	Delete
4	File Exists	5	Submit	Delete
5	File Exists	5	Submit	Delete

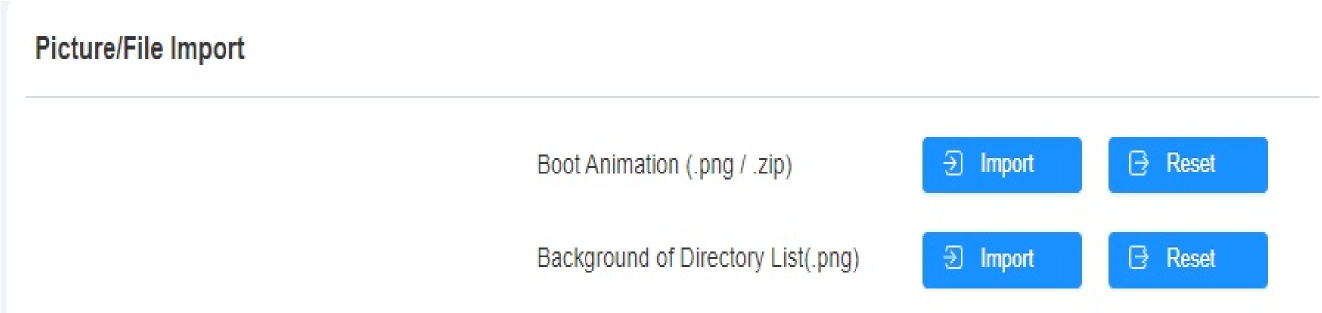
Note

- The pictures uploaded should be in **JPG format** with 2M pixels maximum.
- The recommended resolution is 1080x1920.
- The previous pictures with a specific ID order will be overwritten when the repetitive designation of pictures to the same ID order occurs.

Upload Device Booting Image

You can upload the booting image to be displayed during the device’s booting process if needed.

To configure the configuration on the web **Setting** > **Key/Display** > **Picture/File Import** interface.



Picture/File Import

Boot Animation (.png / .zip)

Background of Directory List(.png)

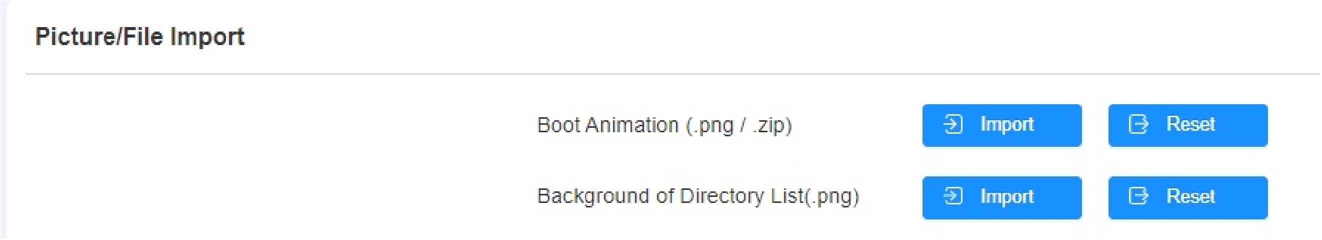
Note

- The pictures uploaded should be in **.png** or **.zip** format.
- The maximum zip file is 20 MB; the maximum png file is 1 MB.
- The recommended resolution is 800*1280.

Upload Device Contact List Background Image

You can customize the background display for the contact list. You can select the picture you like before uploading.

On the web, navigate to **Setting** > **Key/Display** > **Picture/File Import** interface.



Picture/File Import

Boot Animation (.png / .zip)

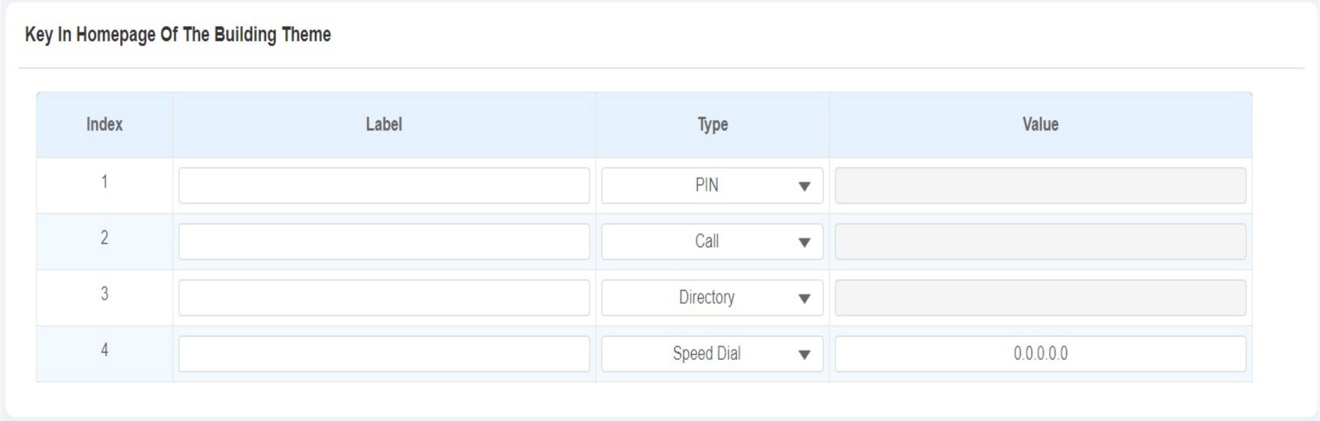
Background of Directory List(.png)

Note

- The pictures uploaded should be in **.png** or **.zip** format.
- The maximum zip file is 20 MB; the maximum png file is 1 MB.
- The recommended resolution is 800x1280.

Home Screen Configuration

You can change the home screen display through the configuration of the tab name and tab arrangement on the device web **Setting > Key/Display > Key In Homepage Of The Building Theme** interface.



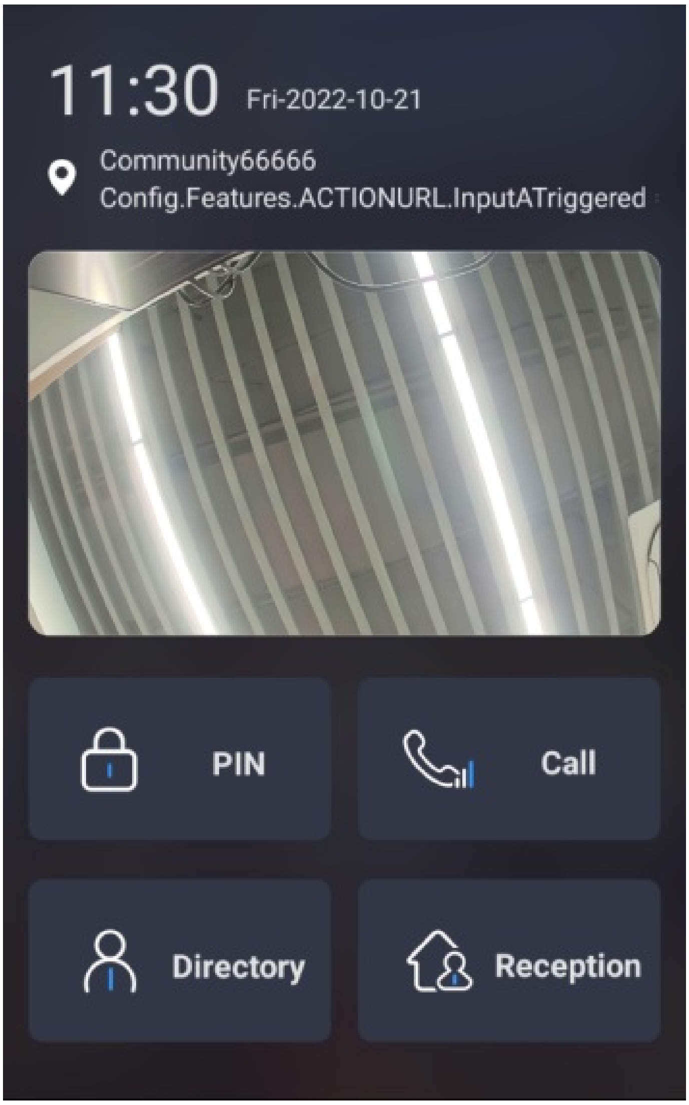
Key In Homepage Of The Building Theme

Index	Label	Type	Value
1		PIN ▼	
2		Call ▼	
3		Directory ▼	
4		Speed Dial ▼	0.0.0.0.0

Configuration for Scenario-based Screen Display Mode

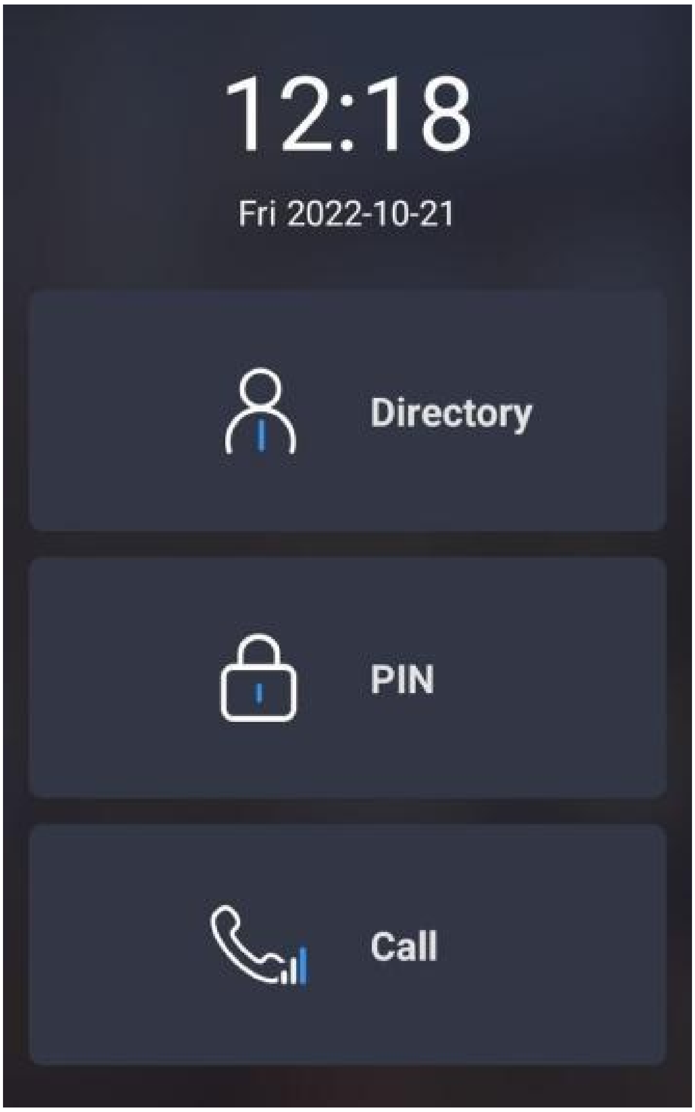
The door phones offer you two types of screen display modes for different applications: Building mode, Villa Mode, and Multi-factor authentication mode.

To set it up, go to **Setting > Key/Display > Theme**.



11:30 Fri-2022-10-21

Community66666
Config.Features.ACTIONURL.InputATriggered



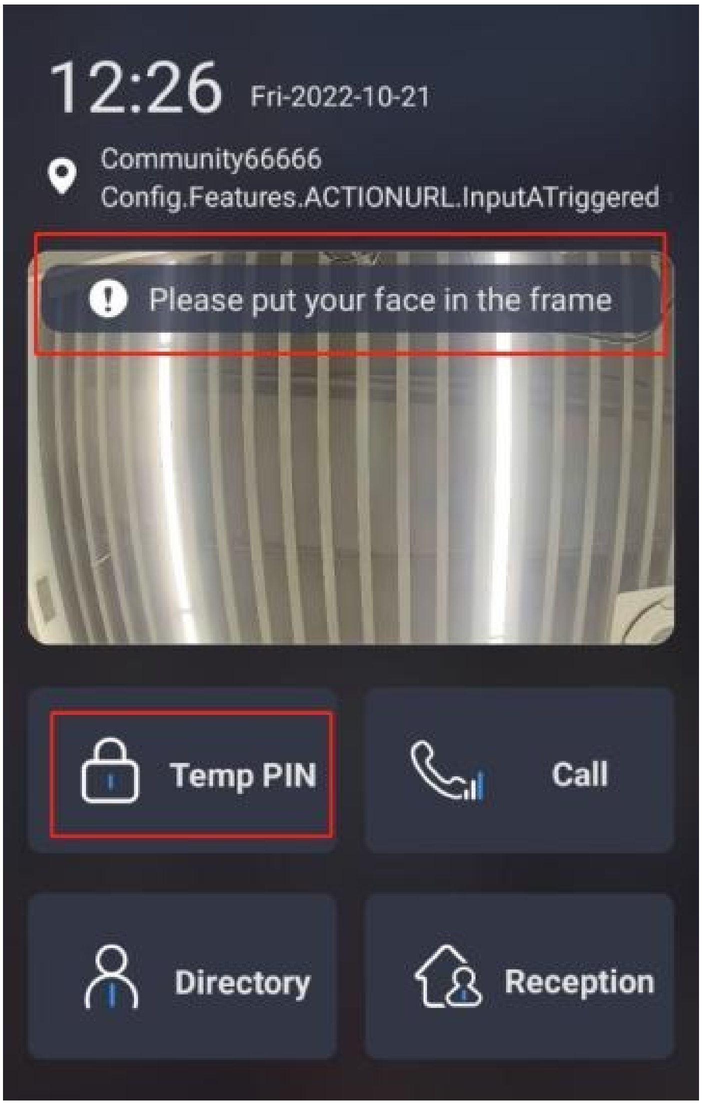
12:18

Fri 2022-10-21

Directory

PIN

Call



12:26 Fri-2022-10-21

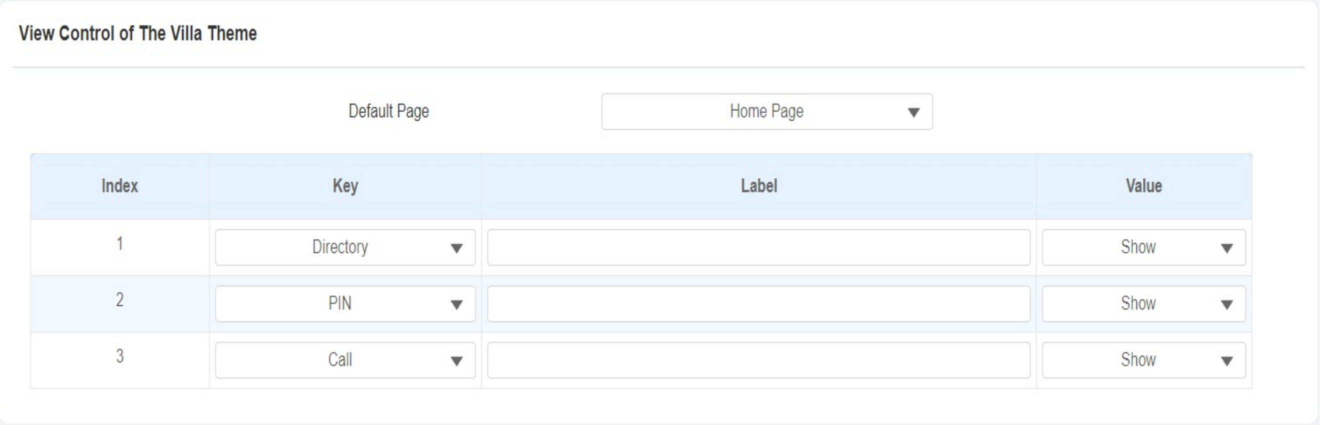
Community66666
Config.Features.ACTIONURL.InputATriggered

Please put your face in the frame

Villa Mode Home Screen Display

You can configure the screen display for the layout of the Tenant icon, PIN icon, and Call icon on the home screen in villa mode.

You can navigate to **Setting> Key/Display > View Control of The Villa Theme** interface.



View Control of The Villa Theme

Default Page: Home Page

Index	Key	Label	Value
1	Directory		Show
2	PIN		Show
3	Call		Show

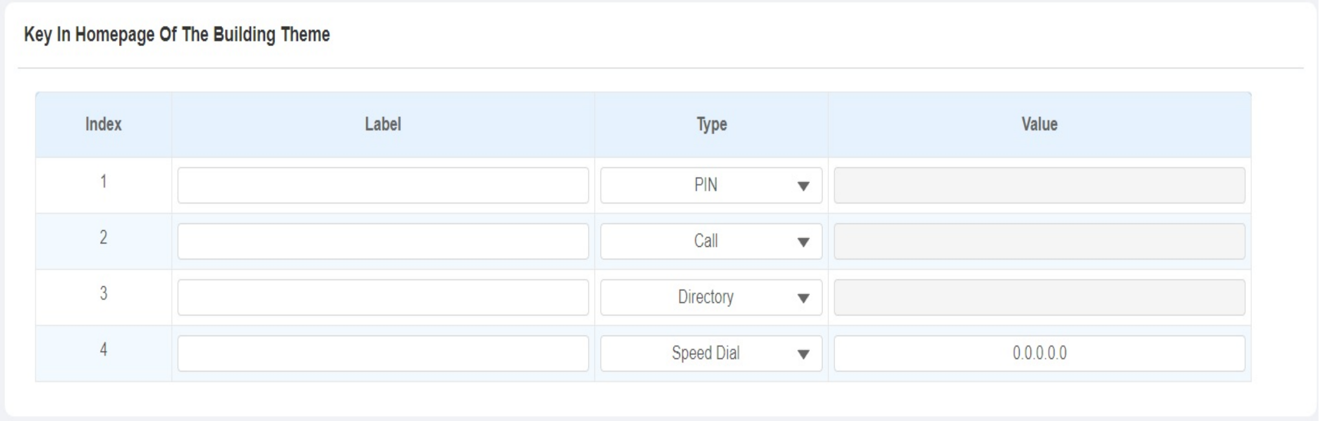
Parameter Set-up:

- **Default Page**: select **Home Page** if you display the tenants, PIN, and Call icon vertically on the home screen. Select Directory if you want to display the contact on the home screen. Select PIN if you want to display the PIN icon with the keypad on the home screen. Select **Call** if you want to display the Call icon with a dial pad on the home screen.
- **Key**: set the type of icon you want to display on the villa mode home screen.
- **Label**: name the icons on the villa mode home screen.
- **Value**: if you set the value as show, the icon will be seen on the screen.

Building Mode Home Screen Display

You can customize your building mode home screen icon display if needed.

To do so, go to **Setting > Key/Display > Key In Homepage Of The Building Theme.**



Key In Homepage Of The Building Theme

Index	Label	Type	Value
1		PIN	
2		Call	
3		Directory	
4		Speed Dial	0.0.0.0.0

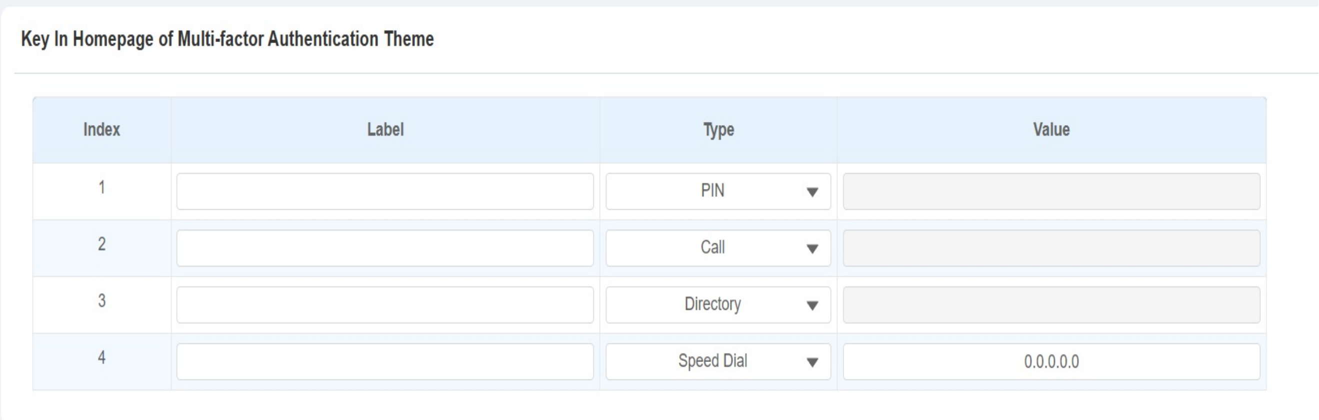
Parameter Set-up:

- **Type**: select the tab type corresponding to the index number which indicates the tab position. For example, if you want to make the **Speed Dial** tab displayed in position one, you can change the type in index number 1 to **Speed Dial.** And you can change another tab position accordingly.
- **Label**: enter a new name to replace the original tab name, but it does not change the attribute of the type.
- **Value**: enter the speed dial number.

Multi-factor Authentication Mode Screen Display

You can also customize your home screen icon display for the multi-factor authentication mode if needed.

To do so, go to **Setting > Key/Display > Multi-factor Authentication Theme** interface.



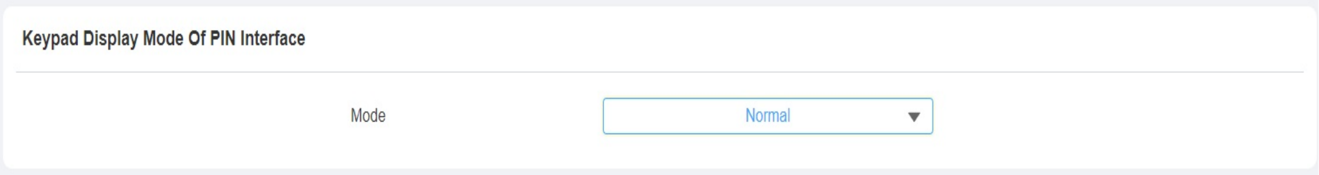
Key In Homepage of Multi-factor Authentication Theme

Index	Label	Type	Value
1		PIN	
2		Call	
3		Directory	
4		Speed Dial	0.0.0.0.0

Dial Key Order

The door phone provides two keypad key display options: Normal and disordered. Opting for the Disordered setting means that the arrangement of keys is randomized each time, enhancing security by preventing password spying.

You can navigate to **Setting > Key/Display> Keypad Display Mode of PIN** Interface.



Keypad Display Mode Of PIN Interface

Mode: Normal

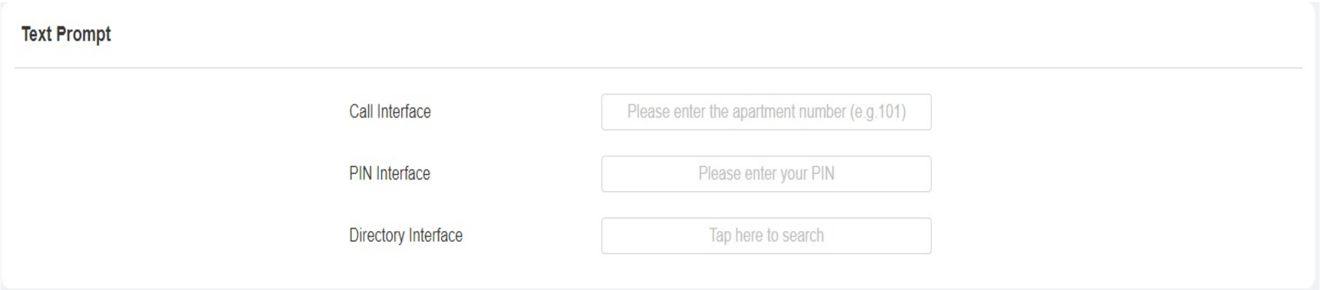
Parameter Set-up:

- **Mode**: select the key order display. Select the disorder key display to better protect your PIN code from being seen by others as you enter the PIN code.

Prompt Display

You can customize your prompts to be displayed on the screen.

To do so, navigate to **Setting > Key/Display > Text Prompt**. Type in the prompt for different screens.



Text Prompt

Call Interface: Please enter the apartment number (e.g.101)

PIN Interface: Please enter your PIN

Directory Interface: Tap here to search

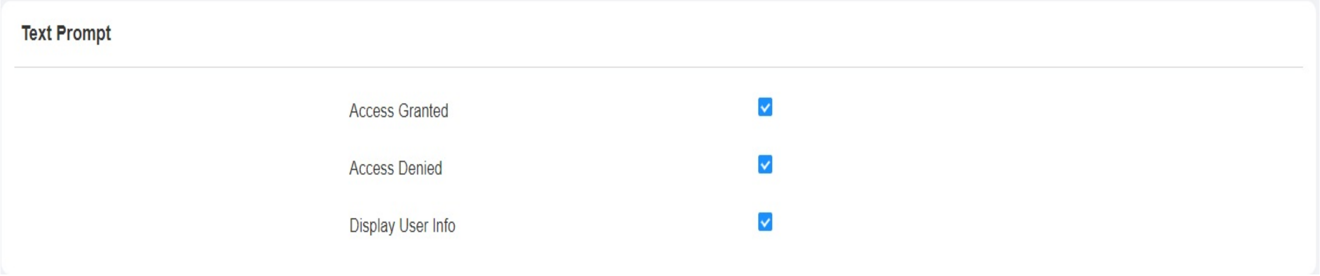
Note

- The door phone supports a 128-digit character maximum in length for the text prompt.

Open Door Text Prompt Display

You can enable the open door text prompt for both door-opening success and failure. And you can also make the door phone display the user information when users use credentials such as RF cards for access.

To do so, navigate to **Access Control > Relay > Text Prompt.**



Text Prompt

Access Granted ☑

Access Denied ☑

Display User Info ☑

Volume and Tone Configuration

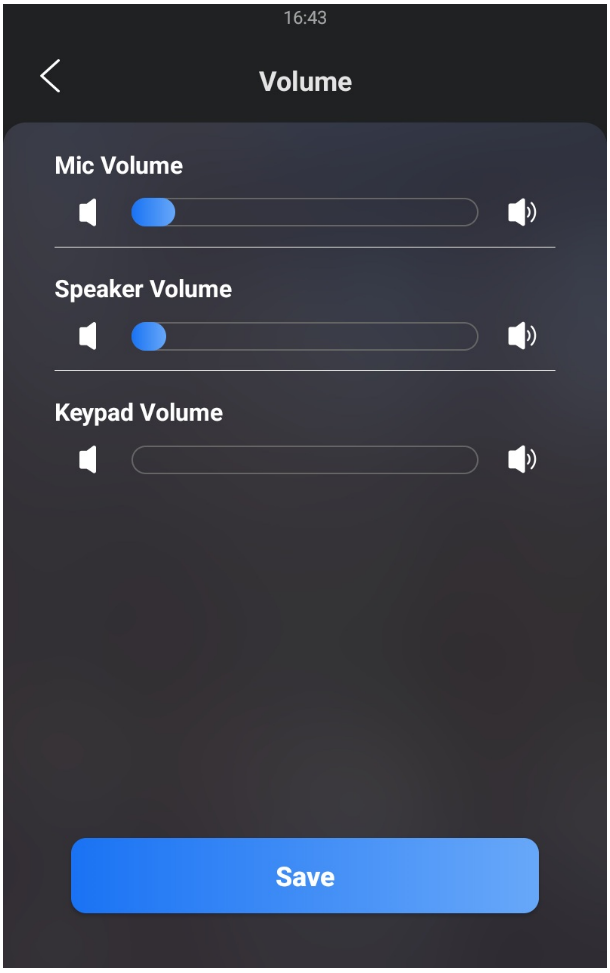
Volume and tone configuration include microphone volume, the AD volume, keypad volume, speaker volume, tamper alarm volume, and open-door tone configuration. Moreover, you can upload the tone you like to enrich your personalized user experience.

Volume Configuration

Configure Volume on the Device

You can adjust the microphone volume, speaker volume, keypad volume, and AD volume on the device.

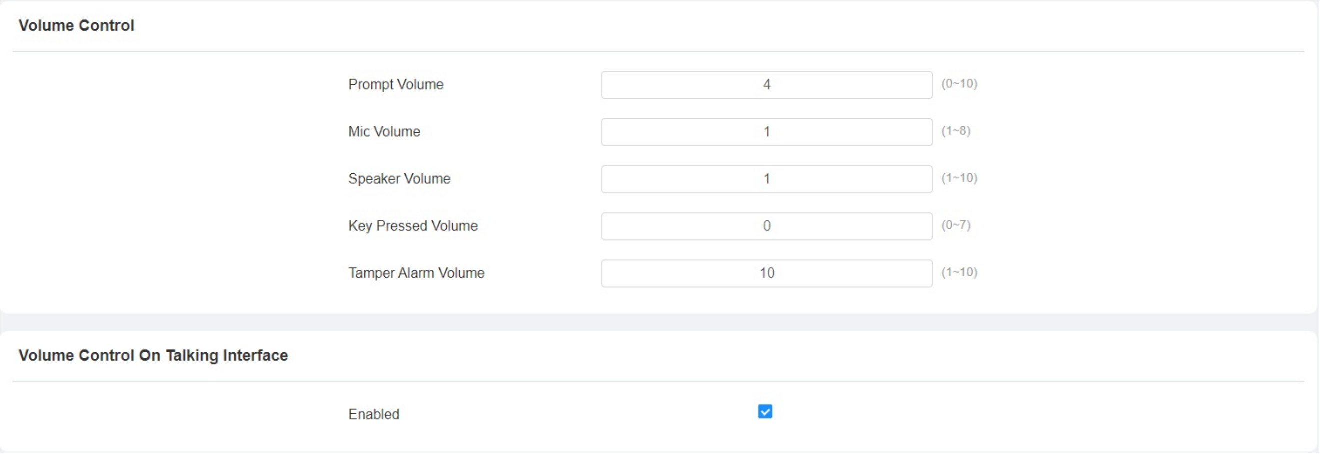
To do so, navigate to **Basic Setting > Volume** interface.



Configure Volume on the Web Interface

On the web interface, you can set the tamper alarm volume, mic volume, etc.

To configure it on the web **Device > Audio** interface.



Volume Control

Prompt Volume	4	(0~10)
Mic Volume	1	(1~8)
Speaker Volume	1	(1~10)
Key Pressed Volume	0	(0~7)
Tamper Alarm Volume	10	(1~10)

Volume Control On Talking Interface

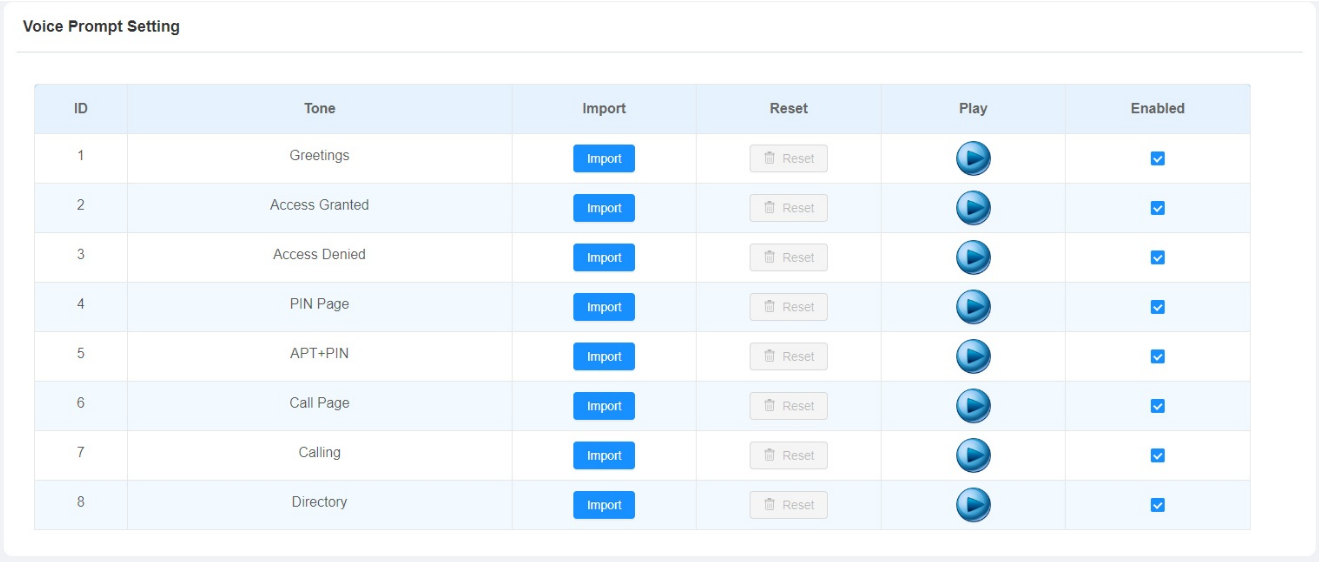
Enabled ☑

Parameter Set-up:

- **Enabled**: tick off the check box if you allow the adjustment to be made on the call volume on the talking screen during a call.

Upload Prompt Tone

You can upload various types of voice prompt. Go to **Device > Audio > Voice Prompt Setting** interface.



Voice Prompt Setting

ID	Tone	Import	Reset	Play	Enabled
1	Greetings	Import	Reset	▶	☑
2	Access Granted	Import	Reset	▶	☑
3	Access Denied	Import	Reset	▶	☑
4	PIN Page	Import	Reset	▶	☑
5	APT+PIN	Import	Reset	▶	☑
6	Call Page	Import	Reset	▶	☑
7	Calling	Import	Reset	▶	☑
8	Directory	Import	Reset	▶	☑

Parameter Set-up:

- **Greetings**: import the greeting tone when the device is booted.
- **Access Granted**: import the prompt tone for door-opening success.
- **Access Denied**: import the prompt tone for door opening failure.
- **PIN Page**: import the prompt tone for the PIN screen.
- **Apart+PIN**: import the prompt tone for the Apartment+ PIN screen.
- **Call page**: import the prompt tone for the call screen.

Note

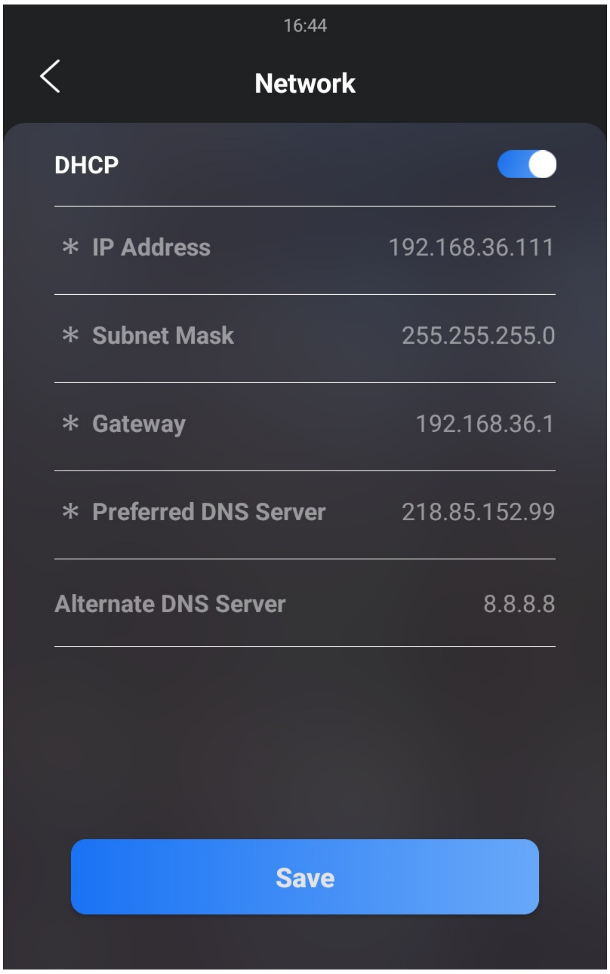
- The open door tone file should be in .wav format and the file size should be smaller than 200KB.

Network Setting

Device Network Configuration

To ensure normal functioning, make sure that the device has its IP address set correctly or obtained automatically from the DHCP server.

To configure on the device **Setting** > **Network** interface.



DHCP	●
* IP Address	192.168.36.111
* Subnet Mask	255.255.255.0
* Gateway	192.168.36.1
* Preferred DNS Server	218.85.152.99
Alternate DNS Server	8.8.8.8

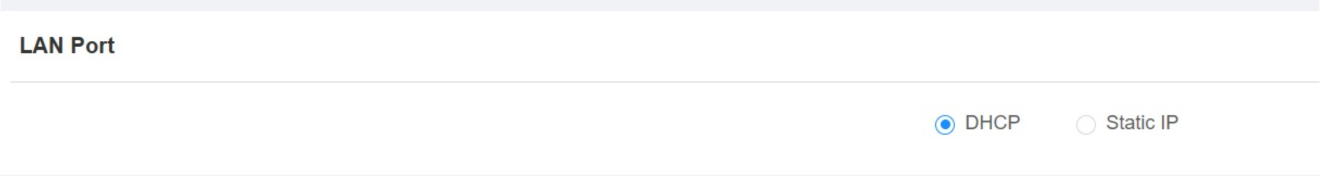
Parameter Set-up:

- **DHCP**: Select the **DHCP** mode by moving the toggle switch to the right. DHCP mode is the default network connection. If the DHCP mode is turned on, then the door phone will be assigned by the DHCP server with an IP address, subnet mask, default gateway, and DNS server address automatically.
- **Static IP**: select the static IP mode by checking off the DHCP check box. When static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS server

address have to be manually configured according to your actual network environment.

- **IP Address**: set up the IP address if the static IP mode is selected.
- **Subnet Mask**: set up the subnet mask according to your actual network environment.
- **Default Gateway**: set up the correct gateway according to the IP address.
- **Preferred & Alternate DNS Server**: set up a preferred or alternate DNS Server (**Domain Name Server**) according to your actual network environment. The preferred DNS server is the primary DNS server address while the alternate DNS server is the secondary server address, and the door phone will connect to the alternate server when the primary DNS server is unavailable.

To configure the configuration on the web **Network > Basic > LAN Port** interface.



LAN Port

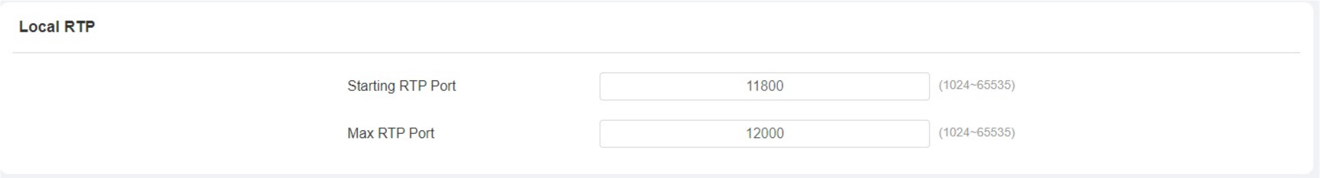
● DHCP ○ Static IP

Device Local RTP Configuration

Real-time Transport Protocol(**RTP**) lets devices stream audio and video data over a network in real time.

To use RTP, devices need a range of ports. A port is like a channel for data on a network. By setting up RTP ports on your device and router, you can avoid network interference and improve audio and video quality.

To configure the configuration on the web **Network > Advanced > Local RTP** interface.



Local RTP

Starting RTP Port	11800	(1024~65535)
Max RTP Port	12000	(1024~65535)

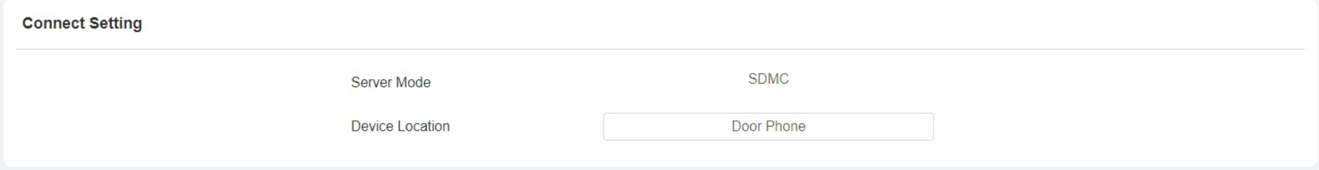
Parameter Set-up:

- **Starting RTP Port**: enter the Port value in order to establish the start point for the exclusive data transmission range.
- **Max RTP port**: enter the Port value in order to establish the end point for the exclusive data transmission range.

Device Deployment in Network

To facilitate device control and management, configure Akuvox intercom devices with details such as location, operation mode, address, and extension numbers.

To configure on the web **Network > Advanced > Connect Setting** interface.



Connect Setting

Server Mode SDMC

Device Location Door Phone

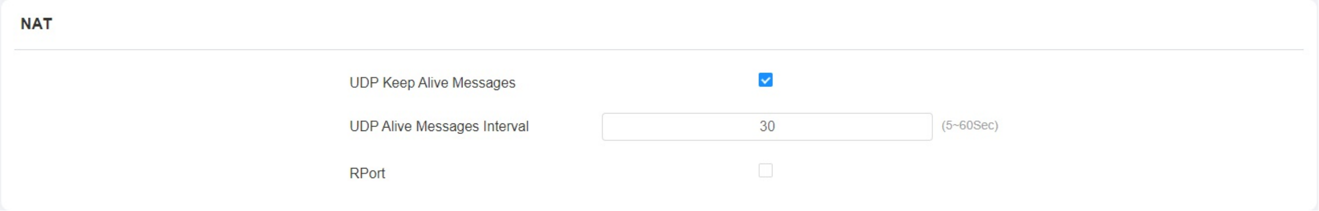
Parameter Set-up:

- **Server Type**: it is automatically set up according to the actual device connection with a specific server in the network such as **SDMC**, **Cloud** or **None. None** is the default factory setting indicating the device is not in any server type. Therefore, you are allowed to choose **Cloud** or **SMDC** in discovery mode.
- **Device Location**: enter the location in which the device is installed and used to distinguish it from other devices.

NAT Setting

Network Address Translation(**NAT**) lets devices on a private network use a single public IP address to access the internet or other public networks. NAT saves the limited public IP addresses, and hides the internal IP addresses and ports from the outside world.

To configure it, go to **Account > Advanced > NAT** interface.



NAT

UDP Keep Alive Messages ☑

UDP Alive Messages Interval 30 (5~60Sec)

RPort □

Parameter Set-up:

- **UDP Keep Alive Messages**: If enabled, the device will send out the message to the SIP server so that the SIP server will recognize if the device is in online status.
- **UDP Alive Messages Interval**: set the message sending time interval from 5-60

seconds, the default is 30 seconds.

- **RPort**: enable the Rport when the SIP server is in WAN (**Wide Area Network**).

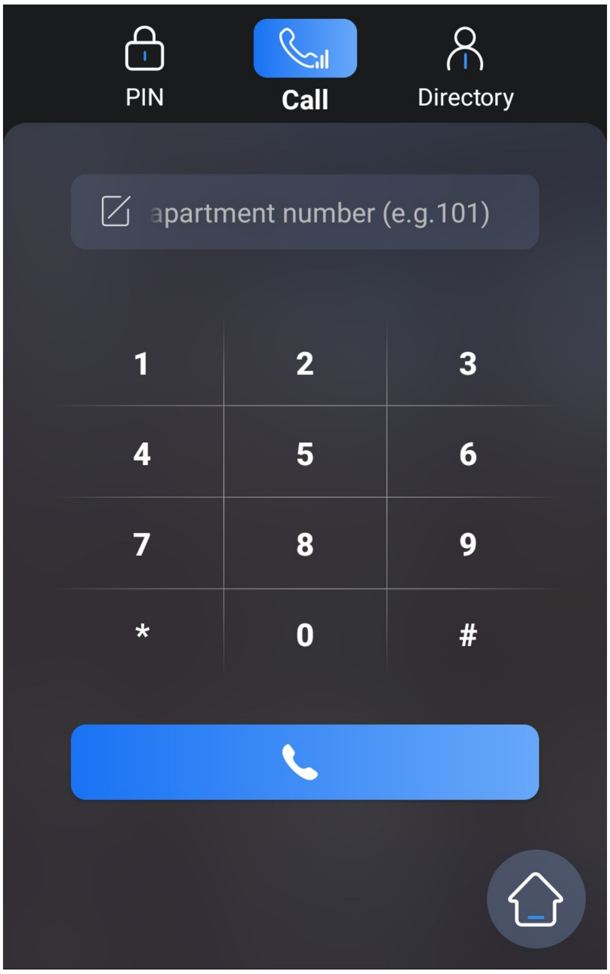
Intercom Call Configuration

IP Call & IP Call Configuration

An IP call is a direct call between two intercom devices using their IP addresses, without a server or a PBX. IP calls work when the devices are on the same network.

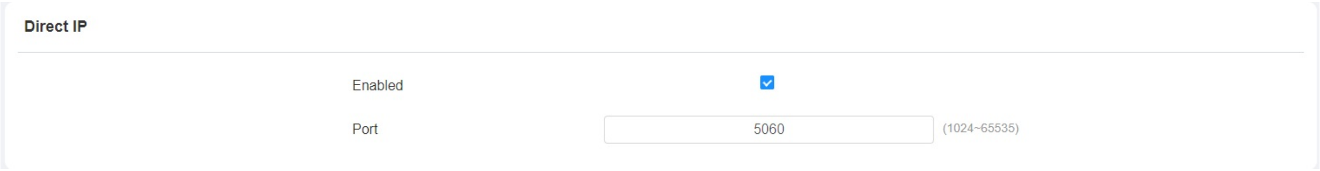
Make IP Calls

To make SIP calls or IP calls on the device by clicking on the dial on the home screen.



IP Call Configuration

To configure the IP direct call on the device **Intercom > Basic > Direct IP** interface.



Direct IP

Enabled ☑

Port 5060 (1024~65535)

Parameter Set-up:

- **Port**: the direct IP Port is **5060** by default with the port range from **1-65535.** When you enter any values within the range other than 5060, you are required to check if the value entered is consistent with the corresponding value on the device you wish to establish a data transmission.

SIP Call & SIP Call Configuration

Session Initiation Protocol(**SIP**) is a signaling transmission protocol used for initiating, maintaining, and terminating calls.

A SIP call uses SIP to send and receive data between SIP devices, and can use the internet or a local network to offer high-quality and secure communication. Initiating a SIP call requires a SIP account, a SIP address for each device, and configuring SIP settings on the devices.

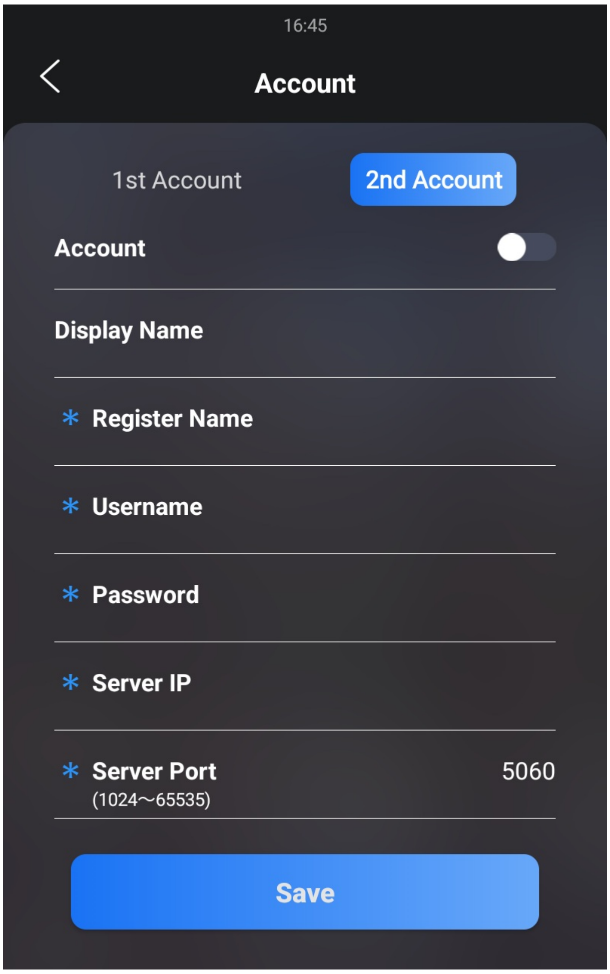
SIP Account Registration

Each device needs a SIP account to make and receive SIP calls.

Akuvox intercom devices support the configuration of two SIP accounts, which can be registered under two independent servers.

Configure SIP Account on the Device

To configure the SIP account on the device **Setting > Account** interface.



16:45

Account

1st Account | 2nd Account

Account ○

Display Name

* Register Name

* Username

* Password

* Server IP

* Server Port (1024～65535) 5060

Save

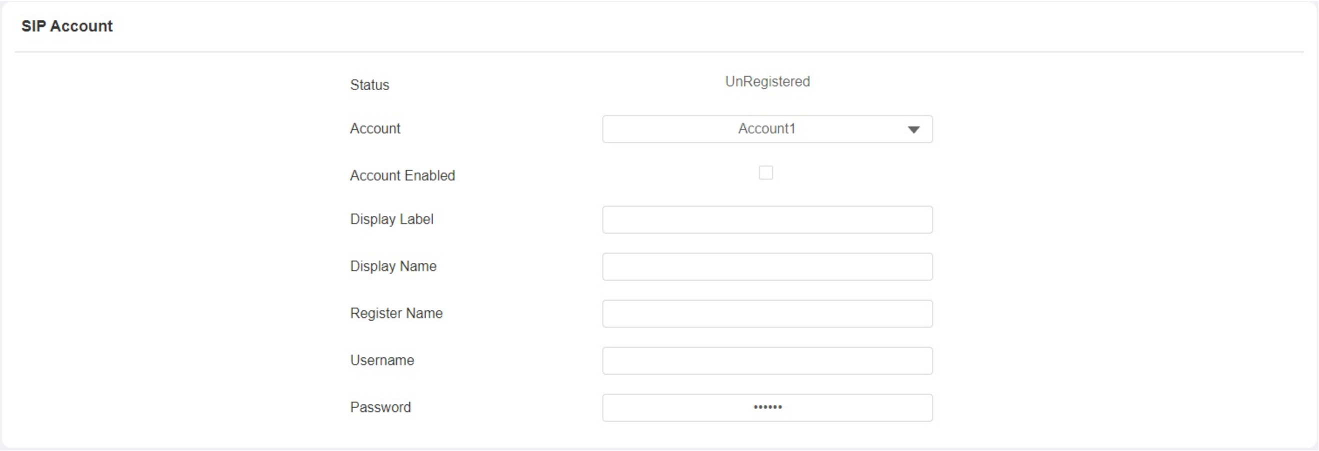
Parameter Set-up:

- **Account**: check to activate the registered account.
- **Display Name**: configure the name, for example, the device’s name to be shown on the device being called to.

a. To register SIP account for Akuvox indoor monitors, obtain **Register Name, Username**, **Password**, **Server IP**, and **Server Port** from Akuvox indoor monitor PBX screen.
b. To register SIP account for third-party devices, obtain **Register Name, Username**, **Password**, **Server IP**, and **Server Port** from third-party service provider.

Configure SIP Account on the Web Interface

To configure the configuration on the web **Account** > **Basic** > **SIP Account** interface.



SIP Account

Status	UnRegistered
Account	Account1
Account Enabled	□
Display Label	
Display Name	
Register Name	
Username	
Password	••••••

Parameter Set-up:

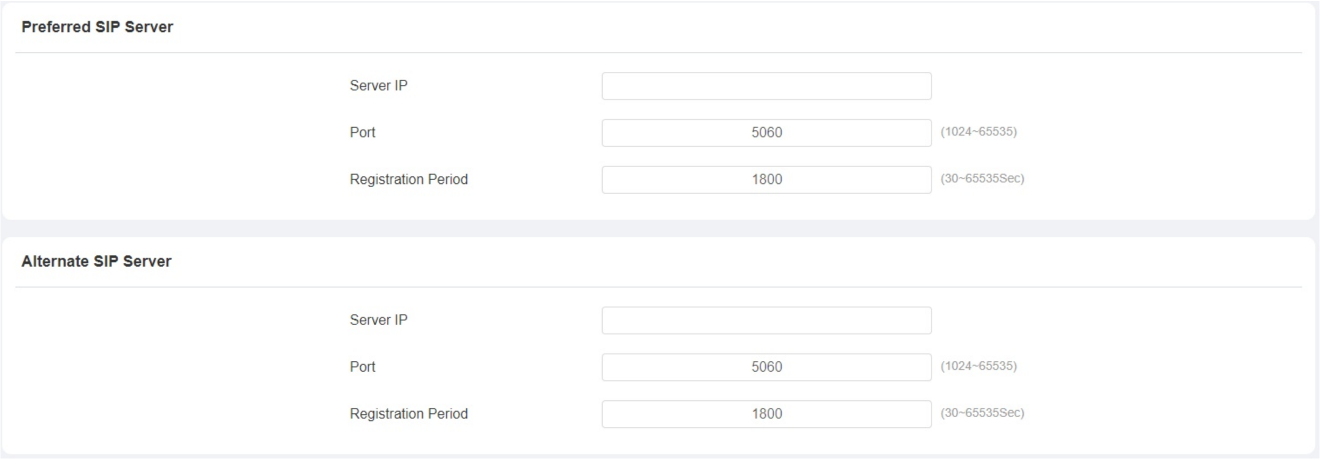
- **Account Active**: click Enable or Disable to activate or deactivate the registered SIP account.
- **Display Name**: configure the name to be shown on the device being called to.
- **Account**: select the exact account (Account 1&2) to be configured.
- **Display Label**: configure the device label to be shown on the device screen.

a. To register SIP account for Akuvox indoor monitors, obtain **Register Name, Username**, and **Password** from Akuvox indoor monitor PBX screen.
b. To register SIP account for third-party devices, obtain **Register Name, Username**, and **Password** from third-party service provider.

SIP Server Configuration

SIP servers enable devices to establish and manage call sessions with other intercom devices using the SIP protocol. They can be third-party servers or built-in PBX in Akuvox indoor monitor.

To configure the configuration on the web **Account > Basic > Preferred SIP Server** interface.



Preferred SIP Server

Server IP		
Port	5060	(1024~65535)
Registration Period	1800	(30~65535Sec)

Alternate SIP Server

Server IP		
Port	5060	(1024~65535)
Registration Period	1800	(30~65535Sec)

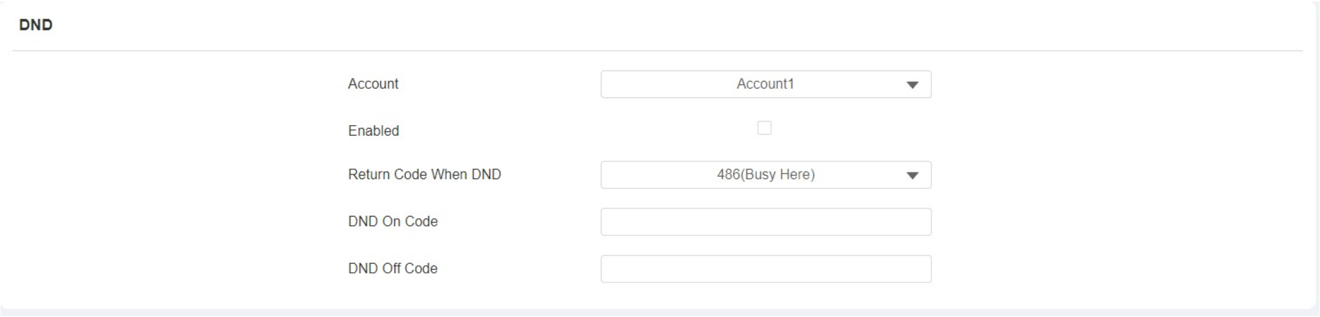
Parameter Set-up:

- **Preferred SIP Server**: enter the primary server IP address number or its URL.
- **Alternate SIP Server**: enter the backup SIP server IP address or its URL.
- **Port**: set up SIP server port for data transmission.
- **Registration Period**: set up 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.

SIP Call DND & Return Code Configuration

The Do Not Disturb(**DND**) feature prevents unwanted incoming SIP calls, ensuring uninterrupted focus. It also allows you to set a code to be sent to the SIP server when rejecting a call.

To configure on the web **Intercom** > **Call Feature** > **DND** interface.



DND

Account	Account1 ▼
Enabled	□
Return Code When DND	486(Busy Here) ▼
DND On Code	
DND Off Code	

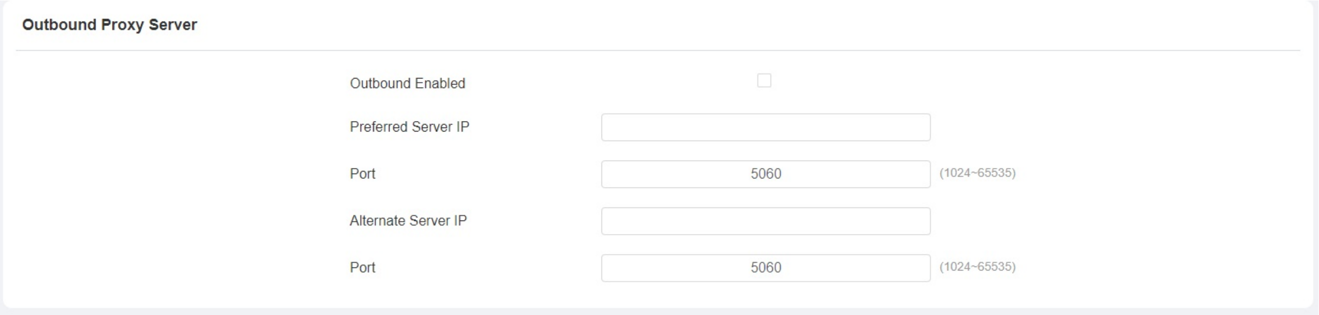
Parameter Set-up:

- **Return Code When DND**: select what code should be sent to the calling device via the SIP server. **404 for Not found; 480 for Temporary unavailable; 486 for Busy Here; 603 for Decline**.

Configure Outbound Proxy Server

An outbound proxy server is used to receive all initiating request messages and route them to the designated SIP server in order to establish a call session via port-based data transmission.

To configure on the web **Account** > **Basic** > **Outbound Proxy Server** interface.



Outbound Proxy Server

Outbound Enabled	□	
Preferred Server IP		
Port	5060	(1024~65535)
Alternate Server IP		
Port	5060	(1024~65535)

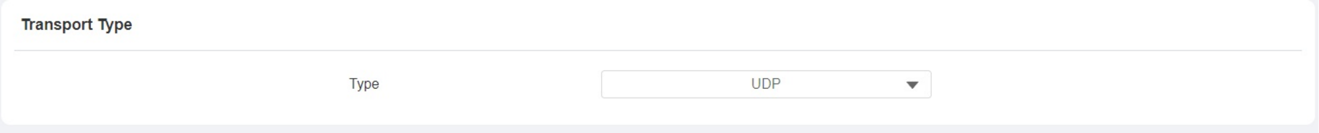
Parameter Set-up:

- **Preferred/Alternate Server IP**: enter the SIP address of the primary/backup outbound proxy server.
- **Port**: enter the Port number for establishing a call session via the primary/backup outbound proxy server.

Configure Data Transmission Type

SIP messages can be transmitted in three data transmission protocols: **UDP** (**User Datagram Protocol**), **TCP** (**Transmission Control Protocol**), **TLS** (**Transport Layer Security**). In the meantime, you can also identify the server from which the data come.

To configure on the web **Account** > **Basic** > **Transport Type** interface.



Transport Type

Type	UDP ▼

Parameter Set-up:

- **UDP**: select **UDP** for an unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
- **TCP**: select **TCP** for a reliable but less-efficient transport layer protocol.
- **TLS**: select **TLS** for a secured and reliable transport layer protocol.

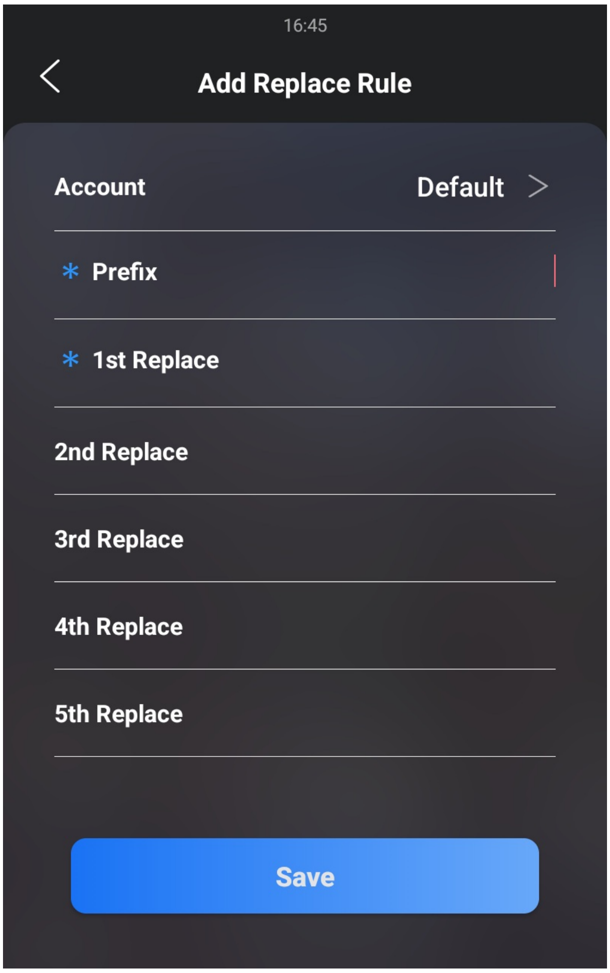
Dial Options Configuration

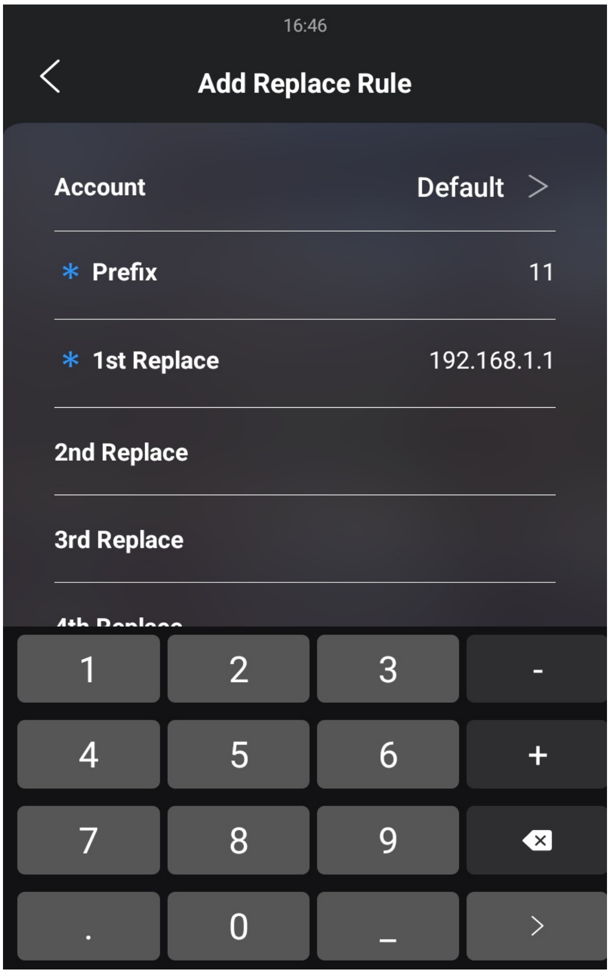
Quick Dial by Number Replacement

The dial number replacement feature simplifies long and complex dial numbers of the device, providing shorter and more user-friendly alternatives for making calls. It allows the substitution of multiple dial numbers, such as IP addresses or SIP numbers, with a single, simplified number.

Quick Dial by Number Replacement on the Device

To configure on the device **Setting > Replace Rule > Add Replace Rule** interface.





Account Default >

* Prefix 11

* 1st Replace 192.168.1.1

2nd Replace

3rd Replace

4th Replace

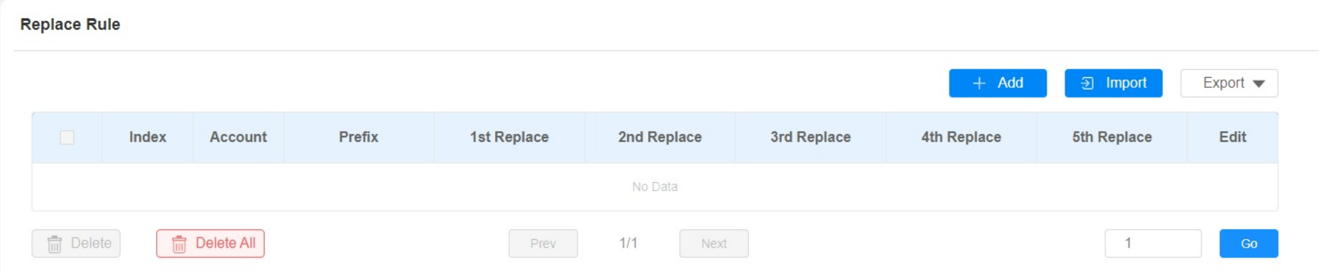
Parameter Set-up:

- **Account**: select the account to which you want to apply dial number replacement. The account is **Auto** by default (to dial out from the account in which the dial number has been registered). You can select either account 1 or account 2 from which the number can be dialed out. if you have registered the dial number in both Account 1 and Account 2, then the number will be called out from Account 1 by default.
- **Prefix**: enter the short number to replace the dial number you wish to replace.
- **Replace 1/2/3/4/5**: enter the dial number(s) you wish to replace. It supports up to 5 numbers maximum for the replacement. For example, if you replace five original dial numbers with a common short number such as **101**, then the five intercom devices with the dial number will be called at the same time when you dial **101**.

Quick Dial by Number Replacement on the Web Interface

You can not only add a quick dial number separately but also import the quick dial number to the device in batch. Besides, you can edit and delete the numbers if needed.

To configure on the web **Intercom > Dial Plan > Replace Rule** interface.



Replace Rule

□	Index	Account	Prefix	1st Replace	2nd Replace	3rd Replace	4th Replace	5th Replace	Edit
No Data									

Note

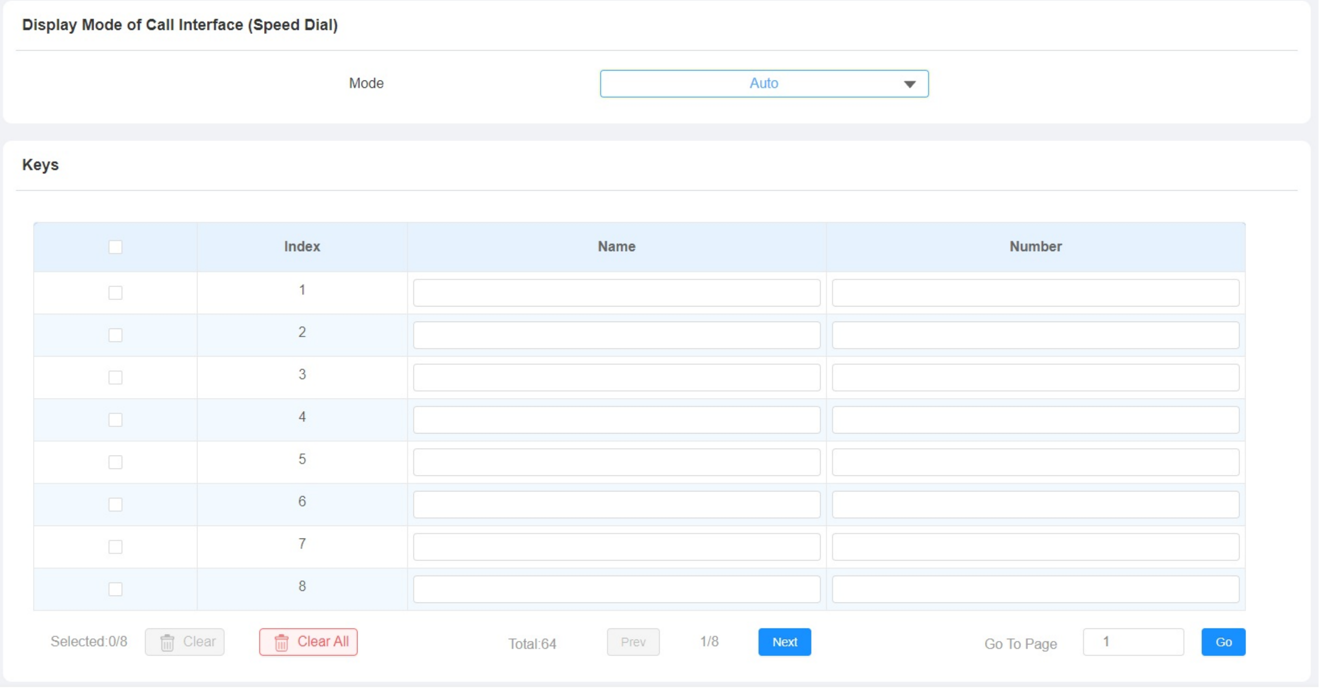
- The check box for each line of **Prefix** should be checked before you can see the **Edit** tab, which you click to carry out the modification.

Speed Dial

Speed Dial in Villa Mode

Speed dial is a function that allows you to create a tab or a combination of organized tabs to be displayed on the device’s dial screen. You can make calls by pressing the specific tabs to make speedy calls without entering any dial numbers.

To configure the speed dial on the web **Setting>Key/Display>Display Mode of Call(Speed Dial)** Interface .



Display Mode of Call Interface (Speed Dial)

Mode: Auto

Keys

□	Index	Name	Number
□	1		
□	2		
□	3		
□	4		
□	5		
□	6		
□	7		
□	8		

Parameter Set-up:

- **Mode**: select the speed dial tab layout among 9 options to your preference. Each option offers you a different layout of dial tabs along with changes to the soft keypad arrangement on the dial screen. The 9 options are explained as follows:

Options	Descriptions
Standard	Select **Standard** if you want to display the time and key pad only with no dial tabs.
Auto	Select **Auto** if you want to select the dial tab layout that does match any one of the other 8 options. For example, if you want to create 3 dial tabs, 5 dial tabs, or 7 tabs, etc., that does not match with other options.
1 Key	Select **1 Key** if you display only one dial tab with no keypad.
1 Key + Keypad	Select **1 Key+Keypad** if you want to display one dial tab with the keypad.
2 Keys + Keypad	Select **2 Keys+Keypad** if you want to display two dial tabs with the keypad.
4 Keys + Keypad	Select **4 Keys+Keypad** if you want to display four dial tabs with the keypad.
8 Keys	Select **8 Keys** if you want to display 8 dial tabs with no keypad.
16 Keys	Select **16 keys** if you want to display 16 dial tabs with no keypad.
64 Keys	Select **64 keys** if you want to display 64 dial tabs with no keypad.

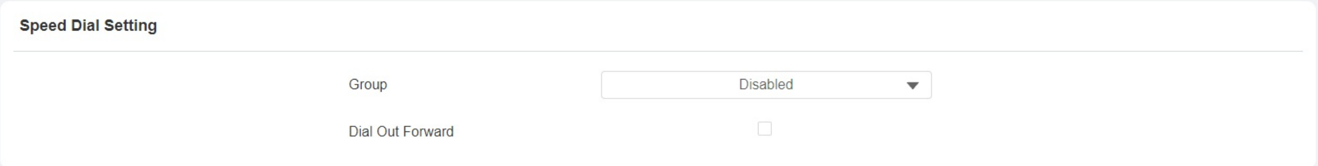
Note

- This function cannot be applied in **Building Mode.**
- The keypad will not be displayed if the number of the dial tabs is over 4 tabs.

Speed Dial in Building Mode

The door phone allows you to call a group of people at the same by pressing the **Reception** button.

On the web, navigate to **Setting > Key/Display > Speed Dial Setting** interface.



Speed Dial Setting

Group: Disabled

Dial Out Forward: □

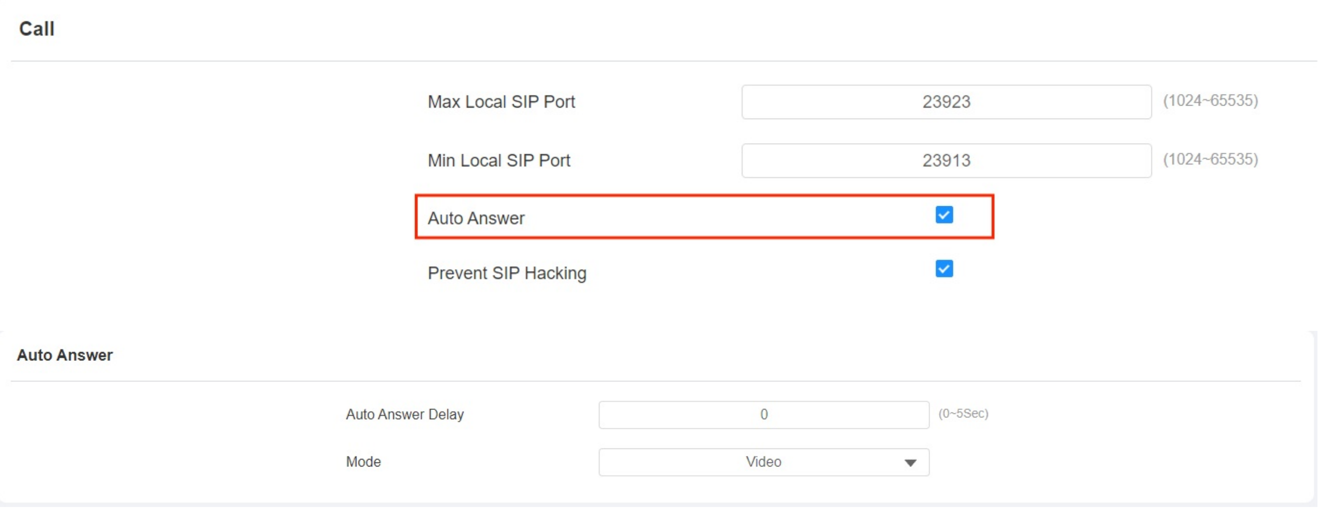
Parameter Set-up:

- **Group**: select the contact group to be called by pressing the Reception button.

Call Auto-answer Configuration

Auto-answer feature allows the device to automatically pick up incoming calls without any manual intervention. You can also customize this feature by setting the time duration for auto-answering and choosing the communication mode between audio and video.

To enable the feature on the web **Account** > **Advanced** > **Call** interface and configure it on the web **Intercom** > **Call Feature** > **Auto Answer** interface.



Call

Max Local SIP Port	23923	(1024~65535)
Min Local SIP Port	23913	(1024~65535)
Auto Answer	☑	
Prevent SIP Hacking	☑	

Auto Answer

Auto Answer Delay	0	(0~5Sec)
Mode	Video	

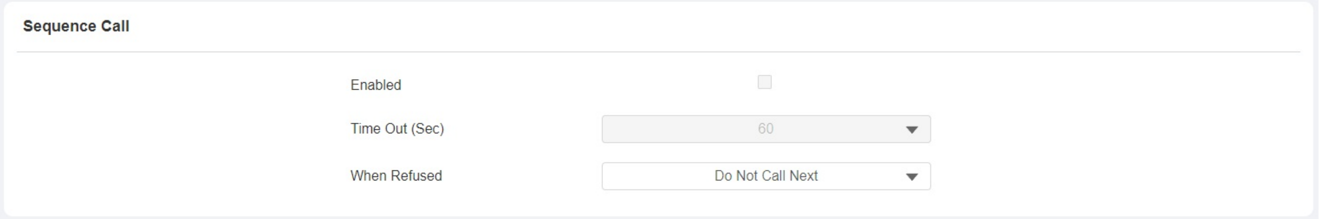
Parameter Set-up:

- **Auto Answer Delay**: set up the delay time (from 0-5s) before the call can be answered automatically. For example, if you set the delay time as 1 second, then the call will be answered in 1 second automatically.
- **Mode**: set up the video or audio mode you preferred for the automatic call answering.

Sequence Call Configuration

Sequence Call is a feature that allows you to dial a group of numbers in a predefined order until one of them answers. This feature is supported by Akuvox SmartPlus, which provides a set of sequence call numbers for the application.

To configure it, go to **Intercom** > **Basic** > **Sequence Call** interface.



Sequence Call

Enabled □

Time Out (Sec): 60

When Refused: Do Not Call Next

Parameter Set-up:

- **Timeout (Sec)**: click to select the call time interval in between the sequence call number in a targeted sequence call group. For example, if you set the time interval as 10 seconds, then the call (if not answered in 10 Sec.) will be terminated automatically and be transferred sequentially to the next sequence call number in the targeted sequence call group.
- **When Refused**: if you select **Do Not Call Next** then the sequence call will be terminated if the call is rejected by the called party. If you select **Call Next** then the sequence call will be continued to the next called party if it is rejected by the first called party.

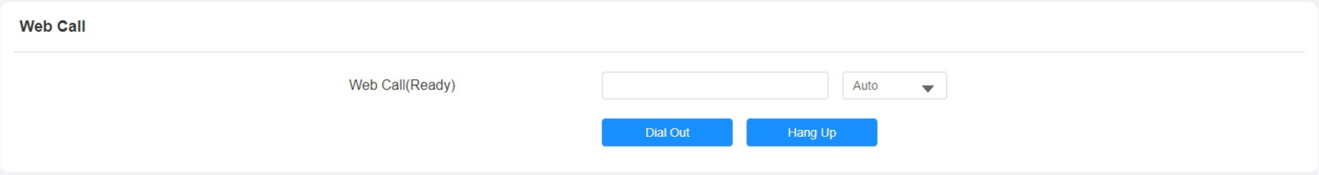
Note

- Sequence Call function should be supported by SmartPlus, please contact Akuvox technical support for more information.

Web Call

The web call feature allows for making calls via the device's web interface, commonly used for remote call testing purposes.

You can navigate to **System > Maintenance > Web Call** interface.



Web Call

Web Call(Ready): Auto

Parameter Set-up:

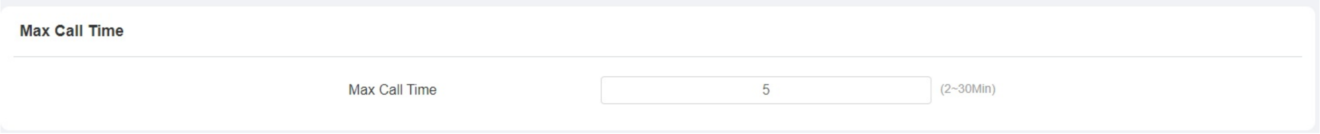
- **Web Call (Ready)**: enter the IP/SIP number to dial out.

Call Settings

Maximum Call Duration Setting

The door phone allows you to set up the call time duration in receiving the call from the calling device as the caller side might forget to hang up the intercom device. When the call time duration is reached, the door phone will terminate the call automatically.

To configure it, go to **Intercom > Call Feature > Max Call Time** interface.



Max Call Time

Max Call Time: 5 (2~30Min)

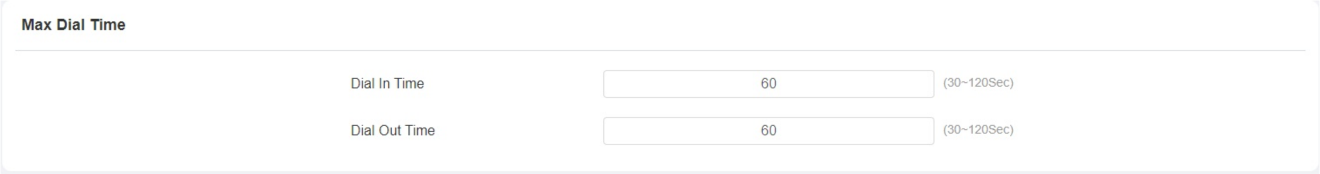
Parameter Set-up:

- **Max Call Time**: enter the call time duration according to your need (ranging from 2-30 min). The default call time duration is 5 min.

Maximum Dial Duration Setting

Maximum Dial Duration is the time limit for incoming- and/or outgoing calls on the door phone. If configured, the door phone will automatically terminate the call if no one answers the call within the preset time, whether it is incoming or outgoing.

To configure on the web **Intercom > Call Feature > Max Dial Time** interface.



Max Dial Time

Dial In Time: 60 (30~120Sec)

Dial Out Time: 60 (30~120Sec)

Parameter Set-up:

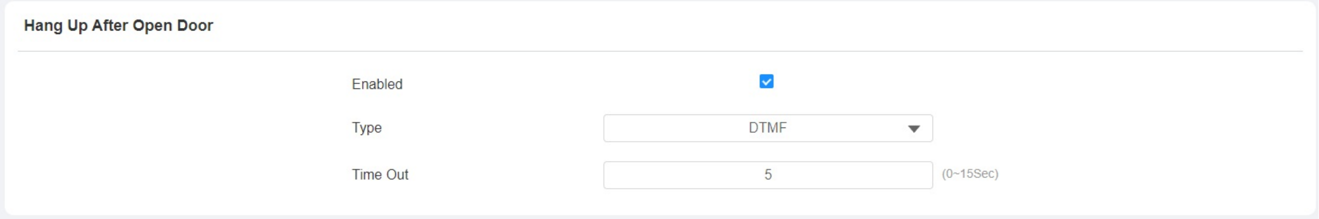
- **Dial In Time**: enter the dial-in time duration for your door phone (ranging from 30-120S) for example, if you set the dial-in time duration is 60 seconds in your door phone, then the door phone will hang up the incoming call automatically if the call is not answered by the door phone in 60 seconds. 60 seconds is the dial-in time duration by default.
- **Dial Out Time**: enter the dial-in time duration for your door phone (ranging from 5-120S)

for example, if you set the dial-out time duration is 60 seconds in your door phone, then the door phone will hang out the call it dialed out automatically if the call is not answered by the device being called.

Hang Up After Open Door

This feature automatically ends the call once the door is released, allowing for the seamless reception of subsequent calls.

To set the feature, go to **Intercom > Call Feature > Hang Up After Open Door** interface.



Hang Up After Open Door

Enabled ☑

Type: DTMF

Time Out: 5 (0~15Sec)

Parameter Set-up:

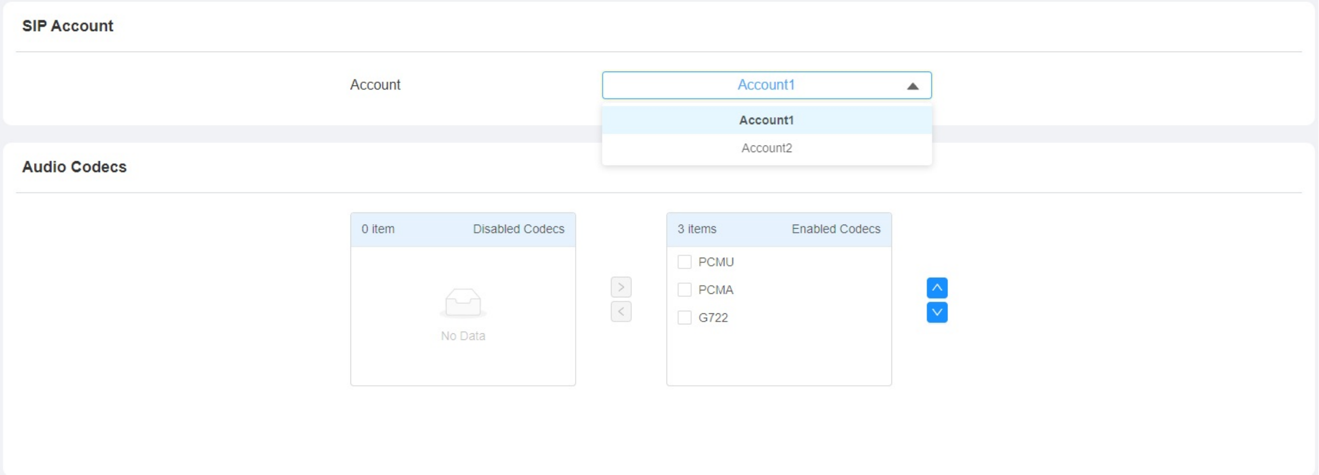
- **Type**: select the open door type. The door can be unlocked via the **DTMF, HTTP** command, **DTMF Or HTTP**, and **DTMF, HTTP or Input**.
- **Timeout**: set up from 1 second to 15 seconds. 5 seconds is the default. If you set it to 5 seconds, then the call will be hung up 5 seconds after the door is opened. If you want to disable the feature, set the timeout as 0.

Audio& Video Codec Configuration for SIP Calls

Audio Codec Configuration

The door phone supports three types of Codec (PCMU, PCMA, and G722) for encoding and decoding the audio data during the call session. Each type of Codec varies in terms of sound quality. You can select the specific codec with different bandwidths and sample rates flexibly according to the actual network environment.

To configure it, go to **Account > Advanced > SIP Account**.



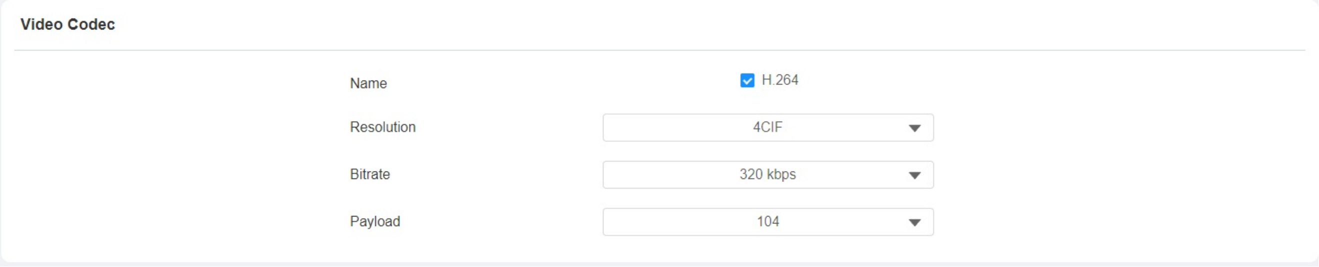
Please refers to the bandwidth consumption and sample rate for the three codecs types below:

Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G722	64 kbit/s	16kHZ

Video Codec Configuration

The door phone supports the H264 codec that provides better video quality at a much lower bit rate with different video quality and payload.

To configure it , go to **Account > Advanced > Video Codec** interface.



Name ☑ H.264
Resolution 4CIF
Bitrate 320 kbps
Payload 104

Parameter Set-up:

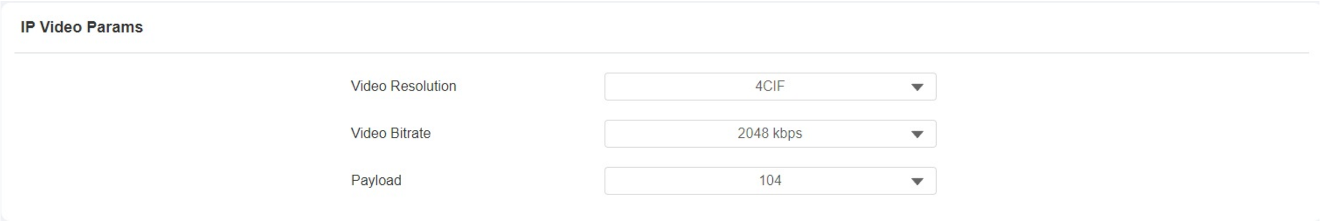
- **Name**: check to select the H264 video codec format for the door phone video. It is enabled by default.
- **Resolution**: select the code resolution for the video quality among five options: **QCIF, CIF, VGA, 4CIF**, and **720P** according to your actual network environment. The default code resolution is **VGA**.
- **Bitrate**: select the video stream bit rate (Ranging from 320-2048). The greater the bitrate,

the data transmitted every second is the greater in amount therefore the video will be clearer. While the default code bitrate is 512 kbps.
- **Payload**: select the payload type (ranging from 90-119) to configure the audio/video configuration file. The default payload is 104.

Video Codec Configuration for IP Direct Calls

You can select the IP call video quality by selecting the proper codec resolution according to the network condition.

To do so, you can go to **Intercom > Call Feature > IP Video Parameters.**



IP Video Params

Video Resolution: 4CIF
Video Bitrate: 2048 kbps
Payload: 104

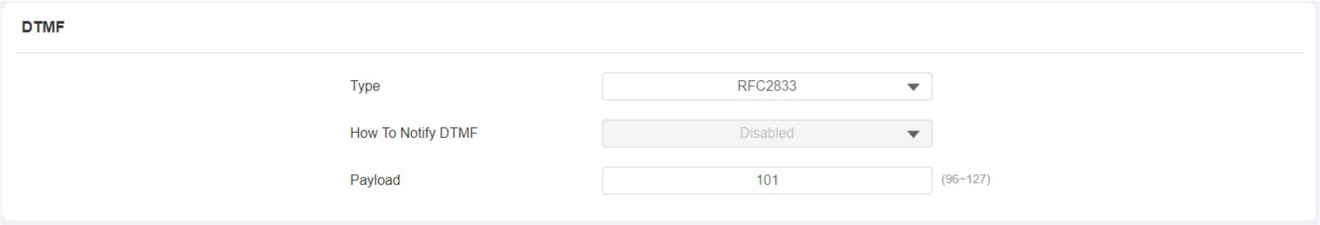
Parameter Set-up:

- **Video Resolution**: select the code resolution for the video quality among four options: **CIF, VGA, 4CIF,** and **720P**. The default code resolution is **720P**.
- **Video Bitrate**: Video Bitrate: select video bit-rate among six options: **128kbps, 256 kbps, 512 kbps, 1024 kbps**, **2048 kbps**, and "**4096kbps**"according to your network environment. The default video bit rate is **2048 kbps**.
- **Video Payload**: select the payload type (ranging from 90-119) to configure the audio/ video configuration file. The default payload is 104.

Configure DTMF Data Transmission

In order to achieve door access via DTMF code or some other applications, you are required to properly configure DTMF in order to establish a DTMF-based data transmission between the door phone and other intercom devices for third-party integration.

To configure it, go to **Account > Advanced > DTMF** interface.



DTMF

Type: RFC2833

How To Notify DTMF: Disabled

Payload: 101 (96~127)

Parameter Set-up:

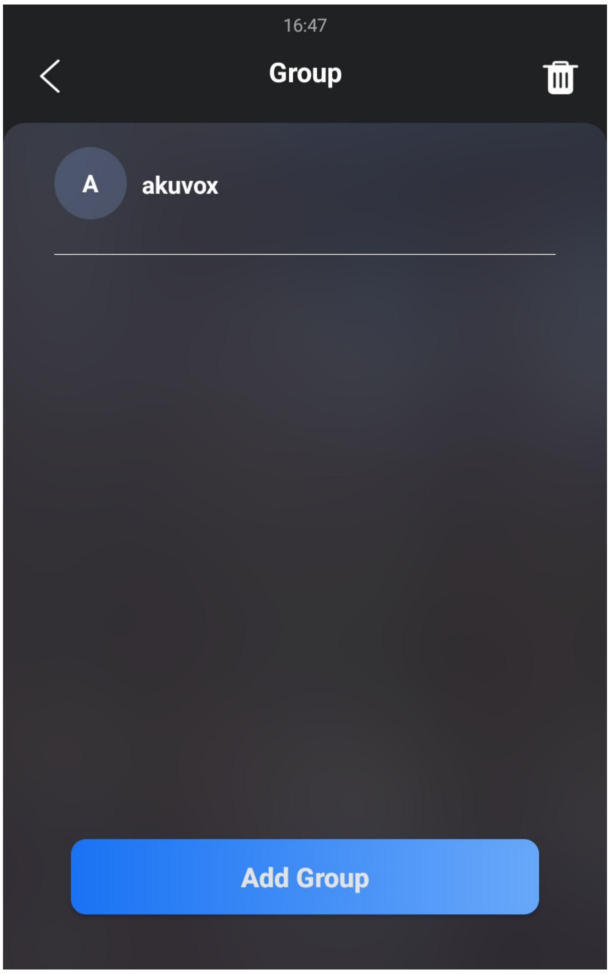
- **Mode**: select DTMF mode among six options: **Inband, RFC2833, Info+Inband, Info**, **Info+Inband+RFC2833**, and **Info+RFC2833** based on the specific DTMF transmission type of the third-party device to be matched with as the party for receiving signal data.
- **How to Notify DTMF**: select among four types: **Disable, DTMF, DTMF-Relay**, and **Telephone-Event** according to the specific type adopted by the third-party device. You are required to set it up only when the third-party device to be matched with adopts **Info** mode.
- **Payload**: set the payload according to the specific data transmission payload agreed on between the sender and receiver during the data transmission.

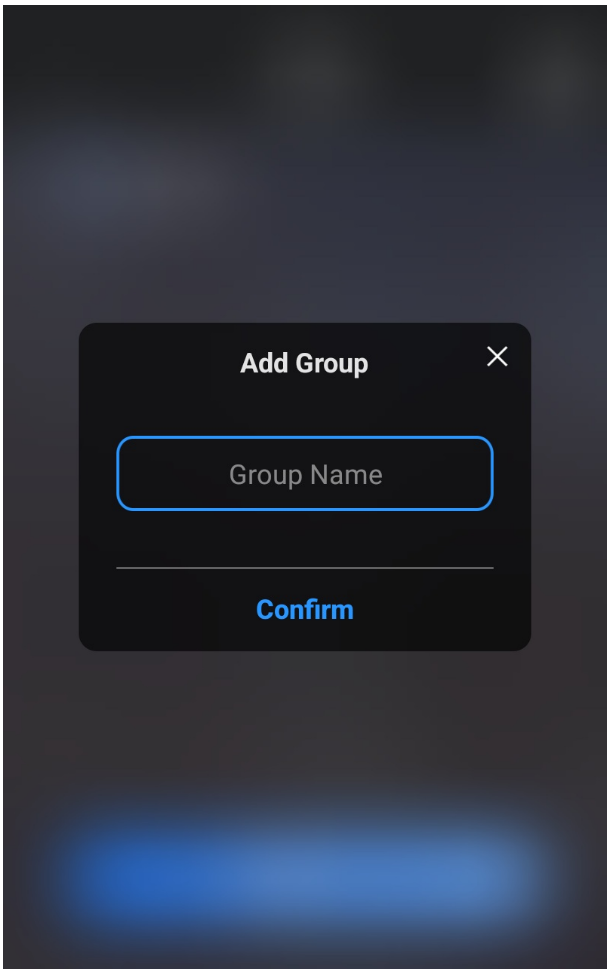
Phone Book Configuration

Phone Book Configuration on the Device

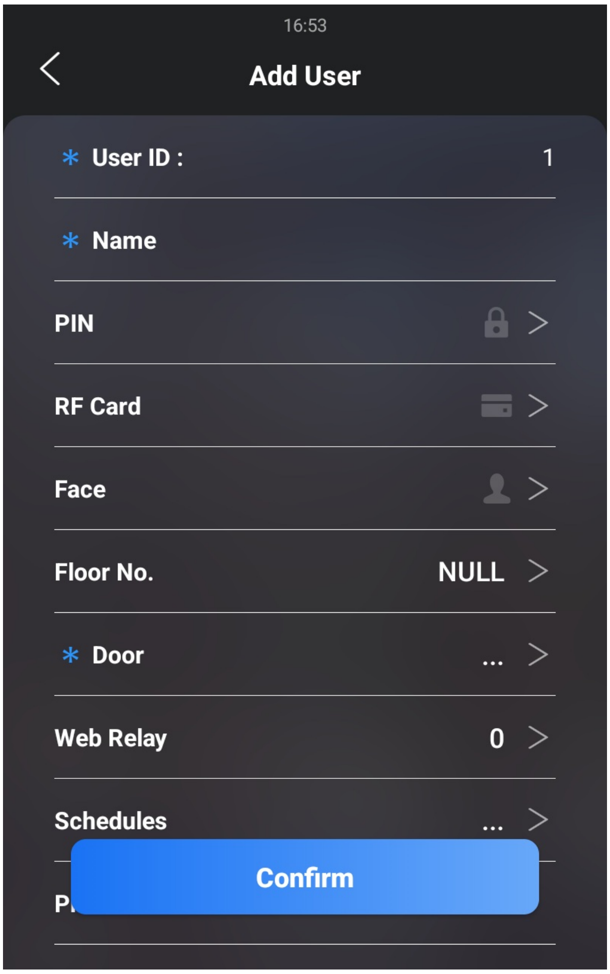
You can create contact groups for users.

Go to **Setting> User > Group** to create a contact group, then go to the **Users List** to configure the contact setting for the users.





Add Group
Group Name
Confirm



16:53

Add User

* User ID :	1
* Name	
PIN	>
RF Card	>
Face	>
Floor No.	NULL >
* Door	... >
Web Relay	0 >
Schedules	... >
P	

Parameter Set-up:

- **Phone**: type in the user's contact number.
- **Group**: select a contact group for the user.

  a. Select the **Default** group if you have not created a contact group for the users.
  b. Select **Hidden Contacts** if you want to hide the contact on the directory screen.
  c. Select a contact group you have created for the users.

- **Dial Account**: select the dial account from which you want to call the contact on the door phone.

Note

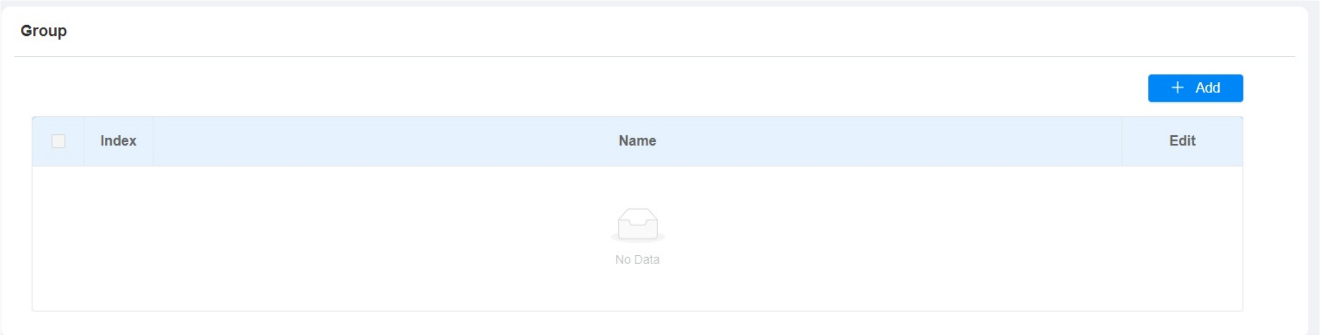
- Only the SIP numbers of the contacts can be called out through the SIP account. IP numbers are not valid for this application.
- A group must be created first before you can select or change the Group.

Phone Book Configuration on the Web Interface

Manage Contact Groups on the Web Interface

You can create and edit a contact group for the contacts. The contact group will be used when you are adding a user.

To create and edit a contact group, go to **Directory > User> Group** interface.



Group

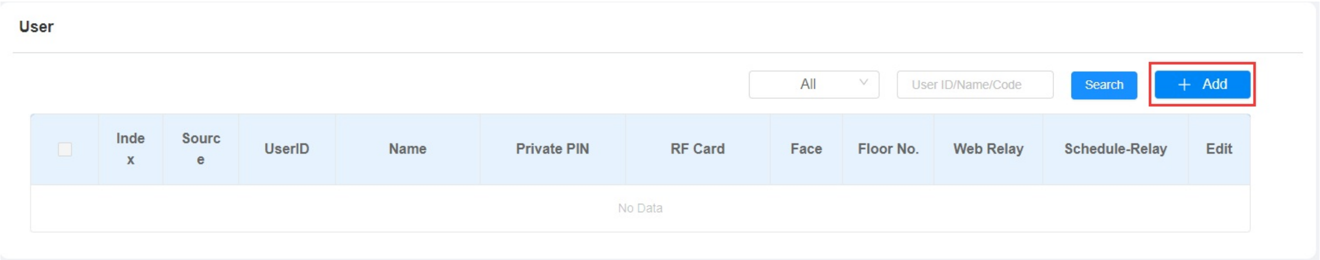
□	Index	Name	Edit

No Data

Contact Configuration for User

You can configure the users' contact settings when adding a user.

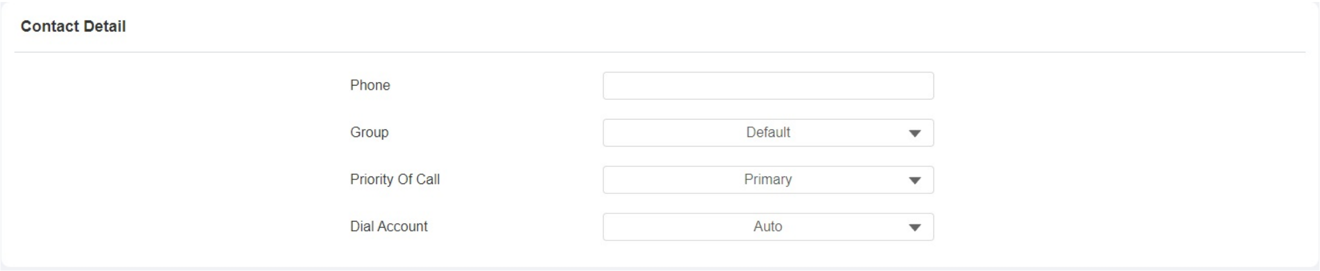
Go to **Directory > User**, click **+Add**, then scroll down to **Contact Detail Setting**.



User

□	Index	Source	UserID	Name	Private PIN	RF Card	Face	Floor No.	Web Relay	Schedule-Relay	Edit

No Data



Contact Detail

Phone	
Group	Default
Priority Of Call	Primary
Dial Account	Auto

Parameter Set-up:

- **Phone**: type in the user's contact number.

- **Group**: select a contact group for the user.

  a. select the **Default** group if you have not created a contact group for the users.
  b. select **Hidden Contacts** if you want to hide the contact on the directory screen.
  c. select a contact group you have created for the users.

- **Priority of Call**: set the call priority for the user in a contact group (Primary, Secondary, and Tertiary) for group calls. for example, if you set it as primary for a user in a selected contact group, then the user will be called first among all the users in the contact group when someone is making a group call.

- **Dial Account**: select the dial account from which you want to call the contact on the door phone.

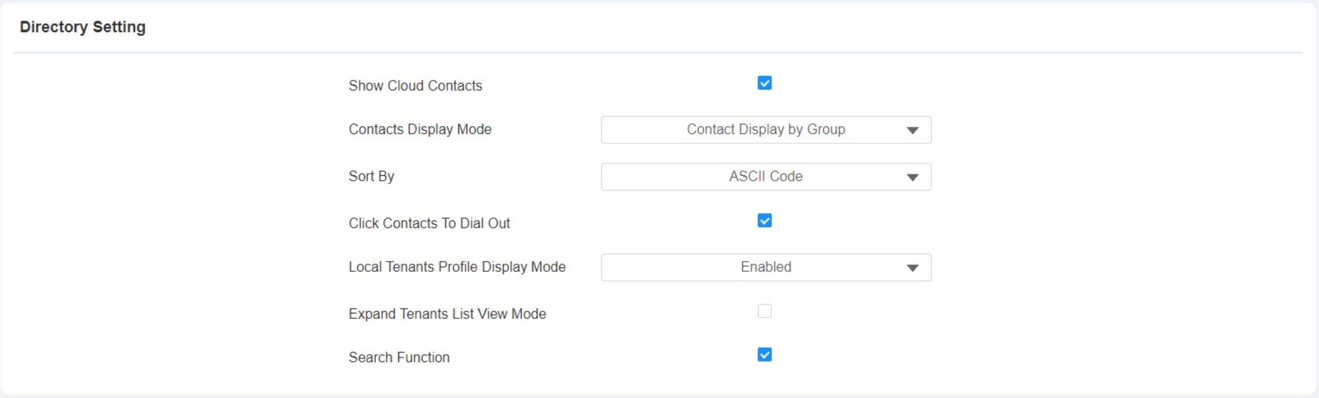
Note

- Priority of Call of a contact cannot be set when the contact does belong to any contact group.
- The contact file format for import should be in .vcf, .csv or .xml format while the contact file format for export should be .vcf format only. And the maximum contact import size is 3000.

Contact List Display Setting

If you want to customize your contact list display to your desired visual preference. You can go to the web interface to do the configuration.

To set it up, go to **Directory > Directory Setting** interface.



Directory Setting

Show Cloud Contacts	☑
Contacts Display Mode	Contact Display by Group
Sort By	ASCII Code
Click Contacts To Dial Out	☑
Local Tenants Profile Display Mode	Enabled
Expand Tenants List View Mode	□
Search Function	☑

Parameter Set-up:

- **Show Cloud Contacts**: tick the check box to show the cloud contacts in the contact list. And when you untick the check box, the cloud contact will be hidden.

- **Contacts Display Mode**: select the contact display mode.

  - If **Group Only** is selected, then all the contact groups will be displayed in order by room number.
  - If **All Contacts** is selected, then all the contacts will be displayed in order by room number.
  - If **Contact Display by Group** is selected, then all the contacts will be displayed in order by ASCII when you unfold the contact group.

- **Sort By**: select **ASCII Code** or **Room No. or Import**. When you select ASCII Code, the tenants will be listed by their names in the sequence of the ASCII code. When you select Room No., the tenants will be sorted according to their room numbers.

- **Click Contacts to Dial Out**: tick the check box to enable the dial-out by pressing the contact tab. When this function is enabled, you can press anywhere on the contact tab to dial out. This function will be disabled when you untick the check box, and when it is disabled, you need to press the **Call** icon in the middle of the tab to dial out.

- **Local Tenants Profile Display Mode**: select **Enabled**, **Disabled** or **Auto**. When the function is enabled, if the tenant has its uploaded contact profile picture, the picture will be displayed next to the name; if not, the default contact icon will be displayed next to the name. When disabled, the picture or the icon will not be displayed. When the function is set as Auto, if the tenant has its uploaded contact profile picture, the picture will be displayed next to the name; if not, there won't be an icon next to the name.

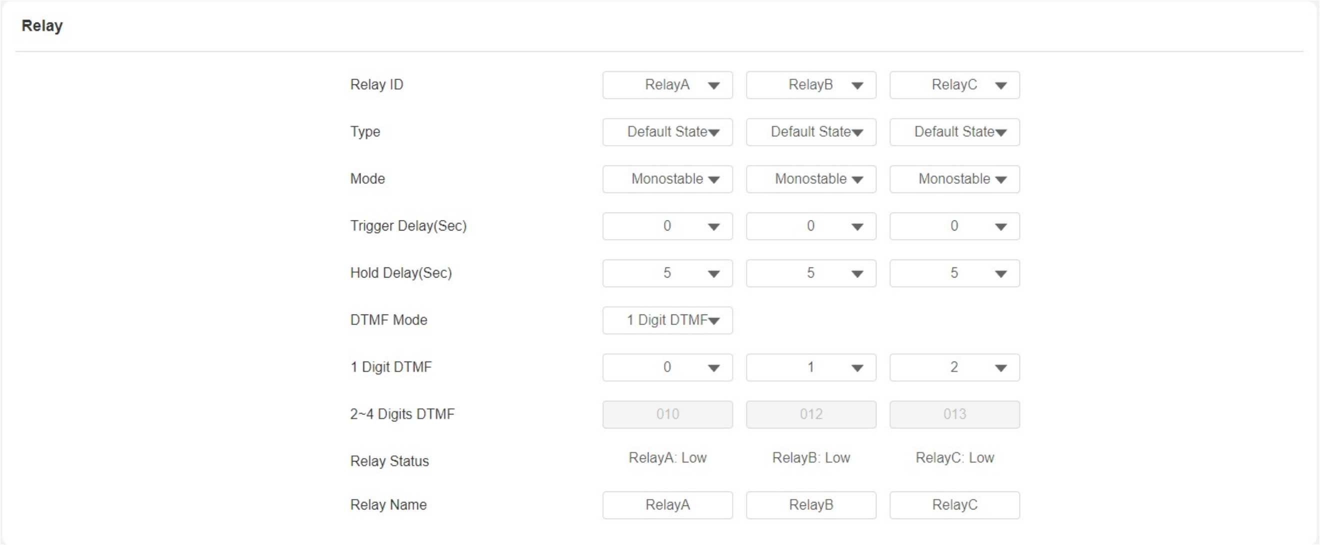
- **Expand Contact List View Mode**: tick the check box to control contact tab size. For example, if you tick the check box then the contact tab will be widened. And the tab will turn to normal size when you untick the check box.

- **Search Function**: tick or untick the check box to control the display of the **Tap here to search** field on the top of the screen. If you untick the check box, then the **Tap here to search** field will be concealed.

Relay Setting

Relay Switch Setting

You can configure the relay switch(es) and DTMF for the door access on the web **Access Control > Relay** interface.



Relay

Relay ID	RelayA	RelayB	RelayC
Type	Default State	Default State	Default State
Mode	Monostable	Monostable	Monostable
Trigger Delay(Sec)	0	0	0
Hold Delay(Sec)	5	5	5
DTMF Mode	1 Digit DTMF		
1 Digit DTMF	0	1	2
2~4 Digits DTMF	010	012	013
Relay Status	RelayA: Low	RelayB: Low	RelayC: Low
Relay Name	RelayA	RelayB	RelayC

Parameter Set-up:

- **Trigger Delay (Sec)**: set the relay trigger delay timing (Ranging from 1-10 Sec). For example, if you set the delay time as 5 Sec. Then the relay will not be triggered until **5** seconds after you press **unlock** tab.
- **Hold Delay (Sec)**: set the relay hold delay timing (Ranging from 1-10 Sec). For example, if you set the hold delay time as **5** Sec. Then the relay will be delayed for 5 seconds after the door is unlocked.
- **DTMF Mode**: select the number of DTMF digits for the door access control (**Ranging from 1-4 digits**) For example, you can select a 1-digit DTMF code or a 2-digit DTMF code, etc., according to your need.
- **1 Digit DTMF**: set the 1-digit DTMF code within range from (**0-9, *, and #**).
- **2~4 Digits DTMF**: set the DTMF code according to the **DMTP Option.** For example, you are required to set the 3-digit DTMF code if **DTMF Mode** is set as 3 digits.
- **Relay Status**: relay status is low by default which means normally closed (NC). If the relay status is high, then it is in Normally Open status (NO).
- **Relay Name**: name the relay switch according to your need. For example, you can name the relay switch according to where the relay switch is located for convenience.

Note

- Only the external devices connected to the relay switch need to be powered by powered adapters as the relay switch does not supply power.
- If DTMF mode is set as **1 Digit DTMF**, you cannot edit the DTMF code in **2~4 Digits DTMF**. And if you set DTMF mode from 2-4 in **2~4 Digits DTMF** field, you cannot edit the DTMF code in the **1 Digit DTMF** field.

Web Relay Setting

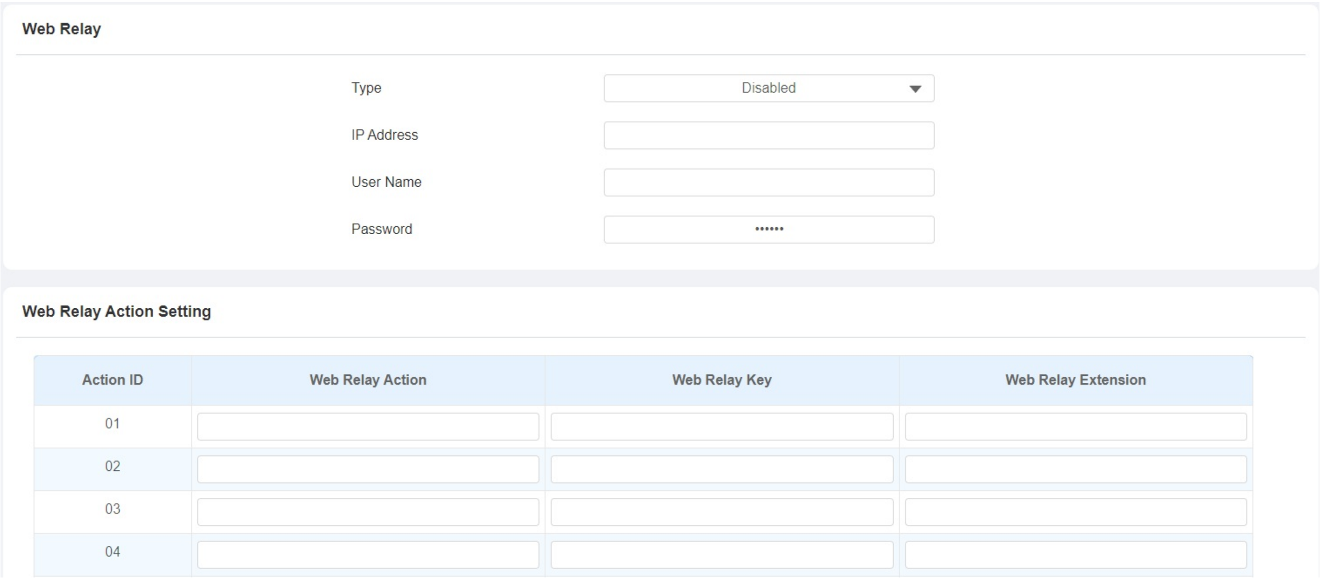
A web relay has a built-in web server and can be controlled via the Internet or a local network. The device can use a web relay to either control a local relay, or a remote relay somewhere else on the network.

Configure Web Relay on the Web Interface

Web relay needs to be set up on the web interface where you are required to fill in such information as relay IP address, password, web relay action, etc. Before you can achieve door access via web relay.

IP address, User Name, and **Password** are provided by the web manufacturer.

To configure it, go to **Access Control > Web Relay** interface.



Web Relay

Type	Disabled
IP Address	
User Name	
Password	••••••

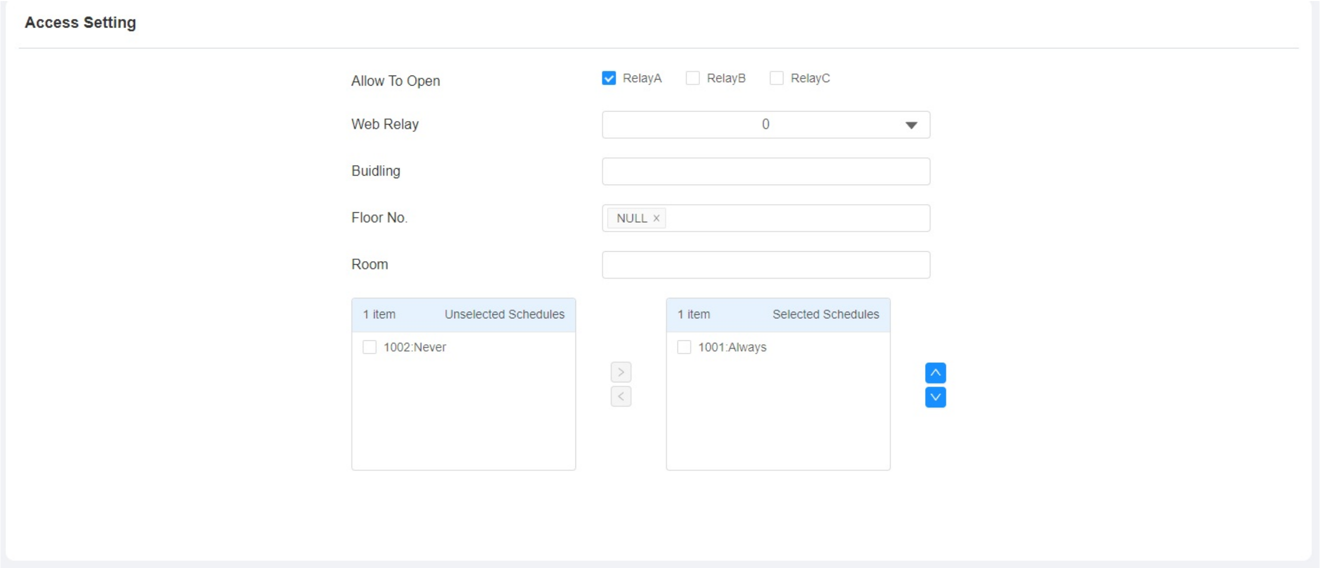
Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
01			
02			
03			
04			

Parameter Set-up:

- **Type**: select among three options **Disabled, Web Relay**, and **Both**. Select **Web Relay** to enable the web relay. Select **Disable** to disable the web relay. Select **Both** to enable both local relay and web relay.
- **Password**: The password is authenticated via HTTP and you can define the passwords using **http get** in Action.
- **Web Relay Action**: enter the specific web relay action command provided by the web manufacturer for different actions by the web relay.
- **Web Relay Key**: enter the configured DTMF code, when the door is unlocked via the DTMF code, the action command will be sent to the web relay automatically.

To select the pre-configured on the web **Directory > User > Add > Access Setting** interface.



Access Setting

Allow To Open	☑ RelayA □ RelayB □ RelayC
Web Relay	0
Buidling	
Floor No.	NULL ×
Room	

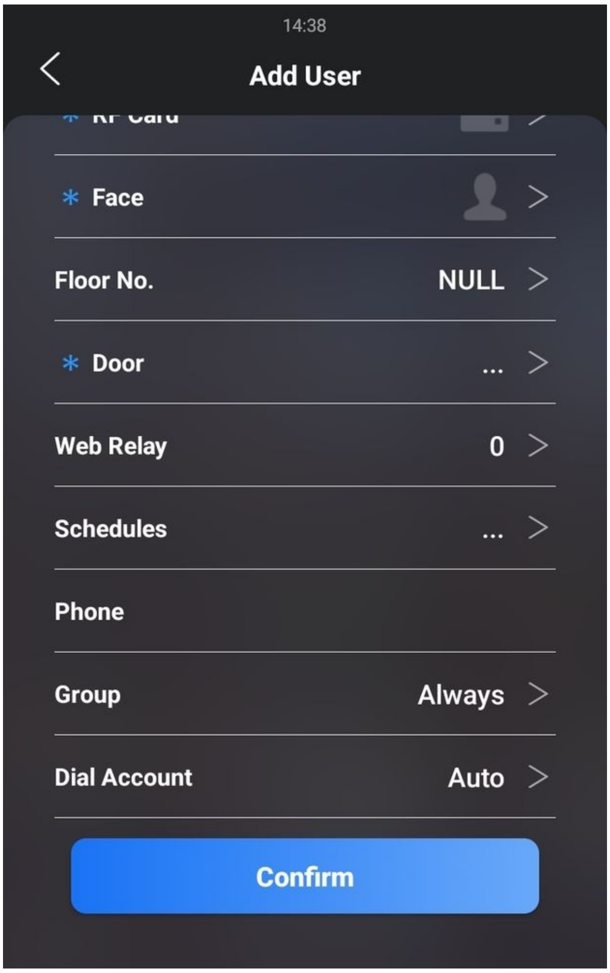
1 item	Unselected Schedules
□ 1002:Never	

1 item	Selected Schedules
□ 1001:Always	

Configure Web Relay Configuration on the Device

You can select the web relay action ID to trigger certain web relay actions, for example for the door opening.

Go to **Setting > User > User List**, then press **Add**.



* RF Card

* Face

Floor No. NULL

* Door ...

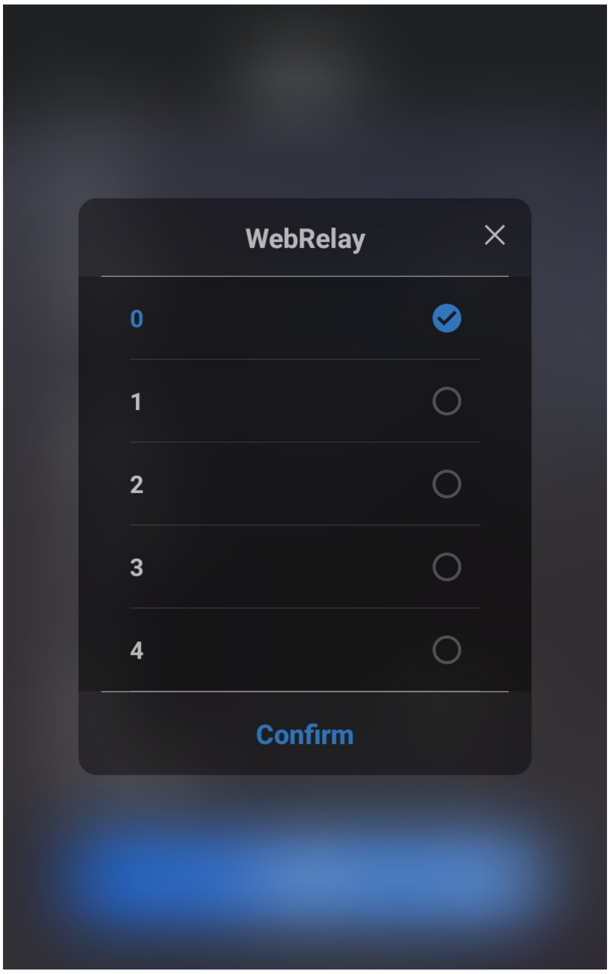
Web Relay 0

Schedules ...

Phone

Group Always

Dial Account Auto



WebRelay ×

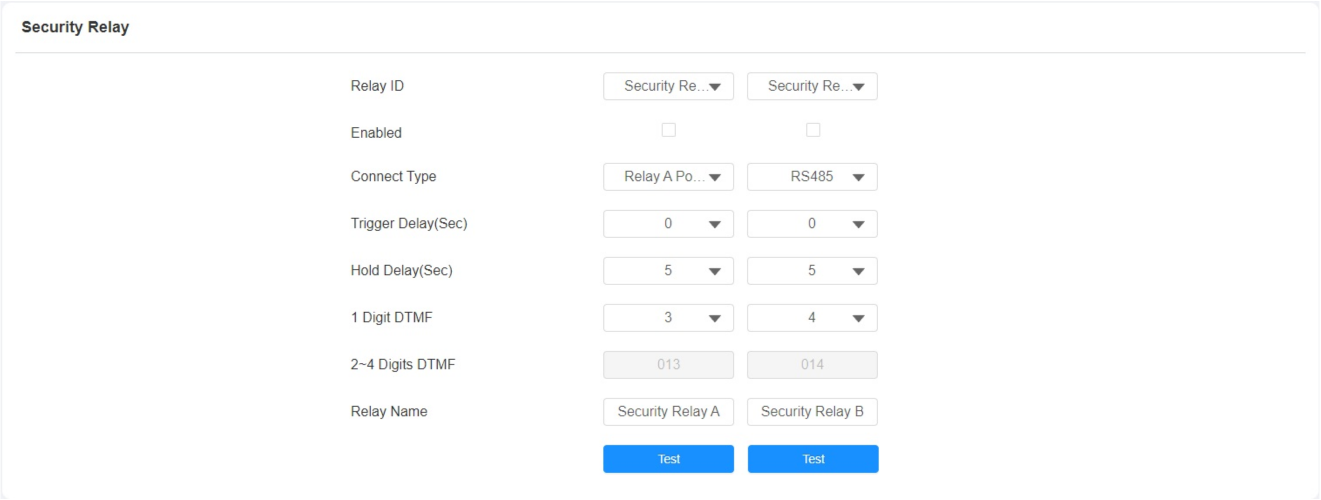
- 0 ✓
- 1 ○
- 2 ○
- 3 ○
- 4 ○

Confirm

Security Relay

The Security Relay, known as Akuvox SR01, is a product designed to bolster access security by preventing unauthorized forced entry attempts. Installed inside the door, it directly governs the door opening mechanism, ensuring that the door remains secure even in the event of damage to the device.

To set up the security relay, navigate to **Access Control** > **Relay** > **Security Relay** interface.



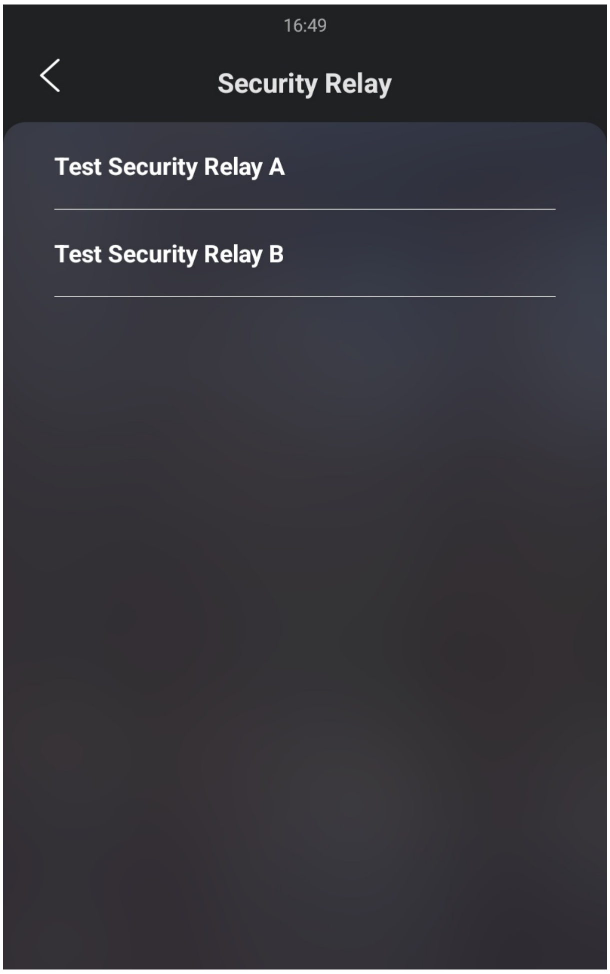
Security Relay

Relay ID	Security Re... ▼	Security Re... ▼
Enabled	□	□
Connect Type	Relay A Po... ▼	RS485 ▼
Trigger Delay(Sec)	0 ▼	0 ▼
Hold Delay(Sec)	5 ▼	5 ▼
1 Digit DTMF	3 ▼	4 ▼
2~4 Digits DTMF	013	014
Relay Name	Security Relay A	Security Relay B
	Test	Test

Parameter Set-up:

- **Connect Type**: select the connection type between the security relay and the door phone. You can select connection via the door phone Relay A Power Output or RS485.
- **Trigger Delay (Sec)**: set the relay trigger delay timing (ranging from 1-10 Sec.) For example, if you set the delay time as 5 sec. then the relay will not be triggered until 5 seconds after you press Unlock tab. The default is 0 meaning triggering relay right after you press the unlock tab.
- **Hold Delay (Sec)**: set the relay hold delay timing (ranging from 1-10 Sec.) For example, if you set the hold delay time as 5 Sec. then the relay will be delayed for 5 after the door is unlocked.
- **1 Digit DTMF**: set the 1-digit DTMF code within range from (0-9 and *,#).
- **2~4 Digits DTMF**: set the DTMF code according to the DMTP Option setting. For example, you are required to set the 3-digit DTMF code if DTMP Mode is set as 3- digits.
- **Relay Name**: give a name to the relay if needed. And relay name can be edited on the SmartPlus cloud and SDMC.

You can also test the security relay on the device, go to **Security > Security Relay**.



16:49

Security Relay

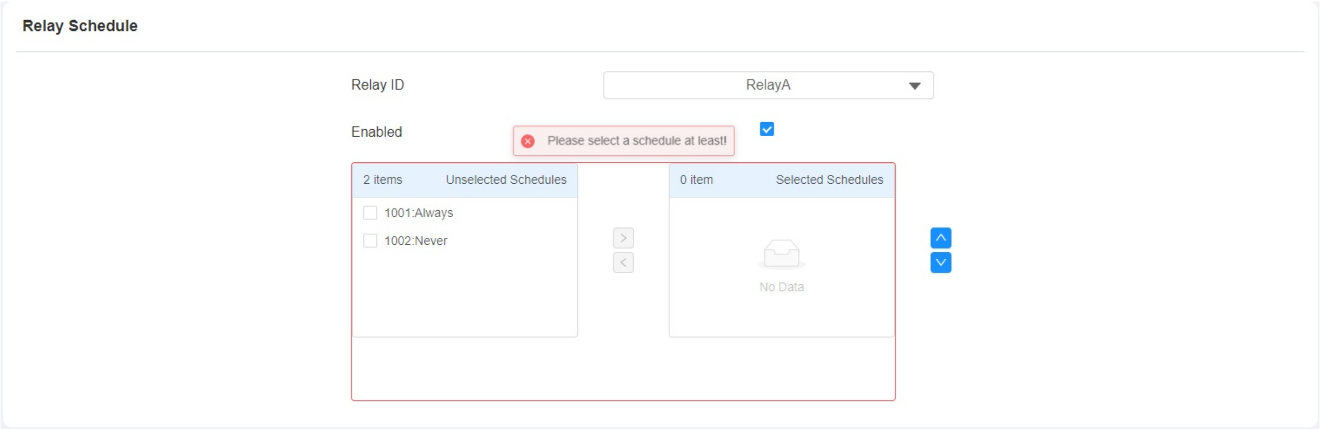
Test Security Relay A

Test Security Relay B

Relay Schedule

The relay schedule allows you to set a specific relay to always open at a certain time. This is helpful for situations like keeping the gate open after school or keeping the door open during work hours.

To do the configuration, navigate to **Access Control > Relay > Relay Schedule** interface.



Relay Schedule

Relay ID: RelayA

Enabled ☑

Please select a schedule at least!

2 items Unselected Schedules
- □ 1001:Always
- □ 1002:Never

0 item Selected Schedules

No Data

Parameter Set-up:

- **Relay ID**: choose the relay you need to set up.
- **Schedule Enabled**: it is disabled by default. Only choose to enable it, and you can select the schedule. For creating the schedule, please refer to the door access schedule configuration.

Note

- You can refer to **Create Door Access Schedule** for the relay schedule setting as the configuration of the relay schedule is identical to the door access schedule.

Door Access Schedule Management

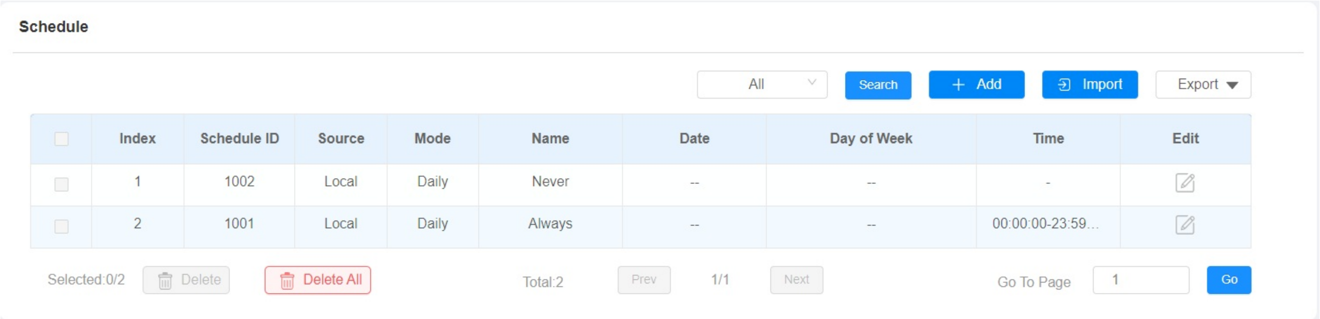
Access Schedule

You can create door access schedules so that they can be later conveniently applied to the door access control intended for individual users or a group of users created. Moreover, you can edit your door access schedule if needed.

Create Access Schedule

You can create the door access schedule on a daily or monthly basis, and you can also create a schedule that allows you to plan for a longer period of time in addition to running the door access schedule on a daily or monthly basis.

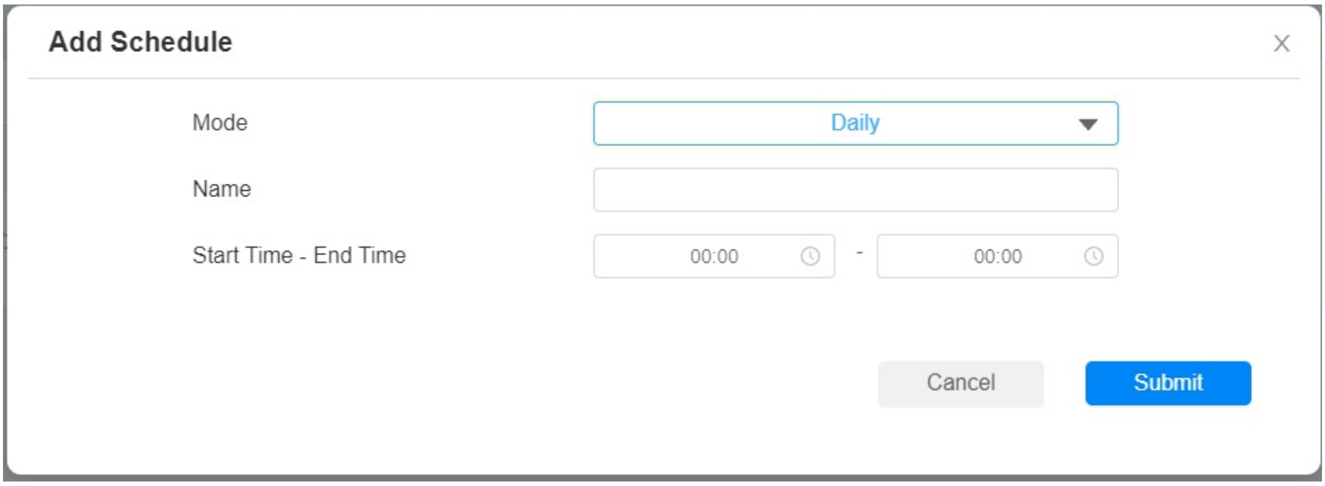
To configure it, go to **Setting > Schedule** interface.



Schedule

□	Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	Edit
□	1	1002	Local	Daily	Never	--	--	-	✎
□	2	1001	Local	Daily	Always	--	--	00:00:00-23:59...	✎

To create a daily schedule, you can do as follows:



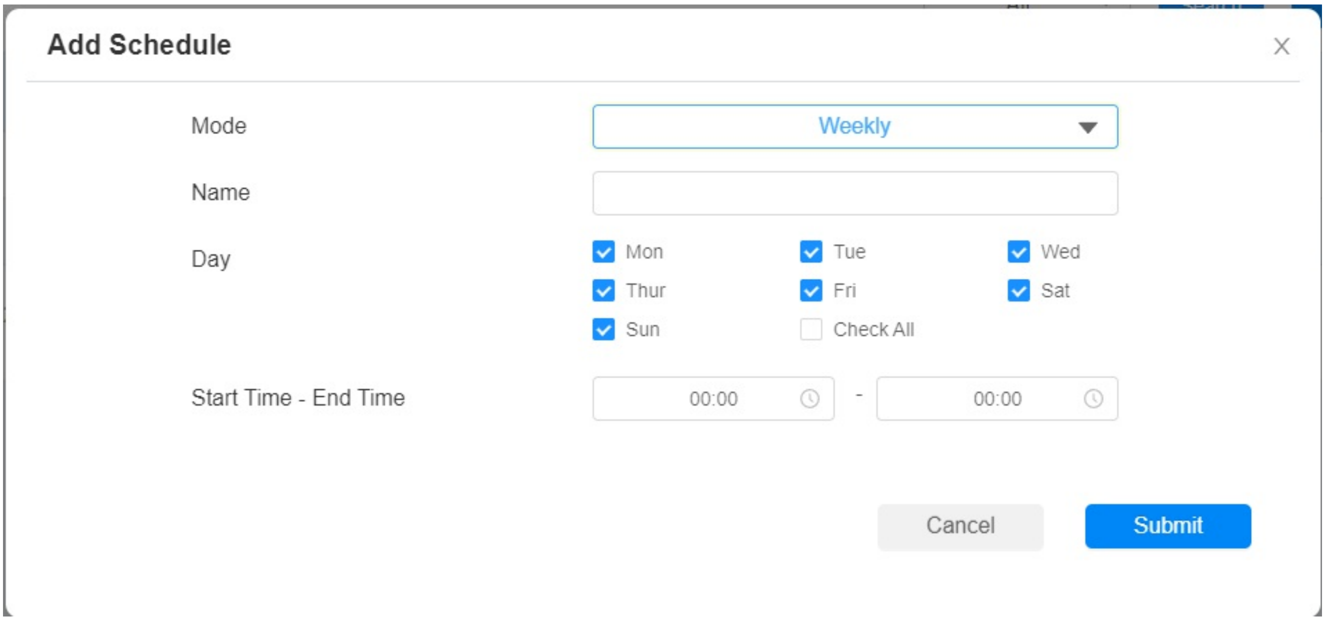
Add Schedule

Mode: Daily

Name:

Start Time - End Time: 00:00 - 00:00

To create a weekly schedule:



Add Schedule

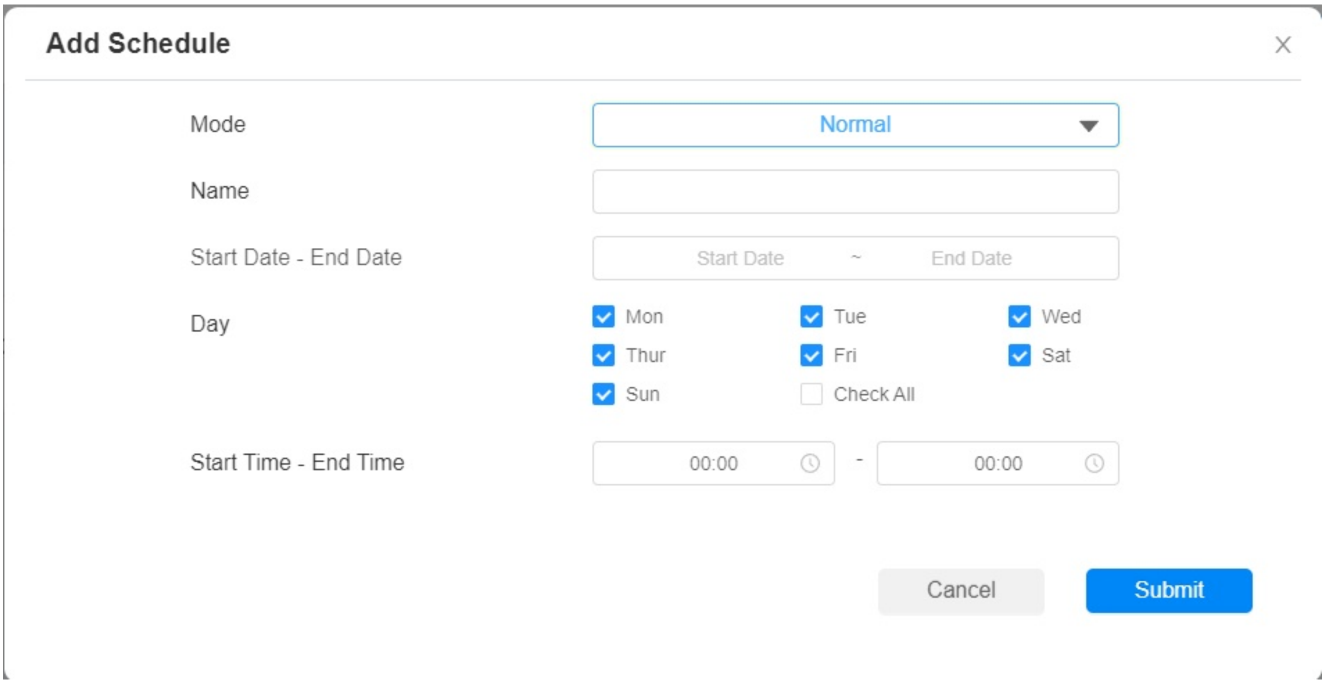
Mode: Weekly

Name:

Day: ☑ Mon ☑ Tue ☑ Wed ☑ Thur ☑ Fri ☑ Sat ☑ Sun □ Check All

Start Time - End Time: 00:00 - 00:00

To create a longer period schedule:



Add Schedule

Mode: Normal

Name:

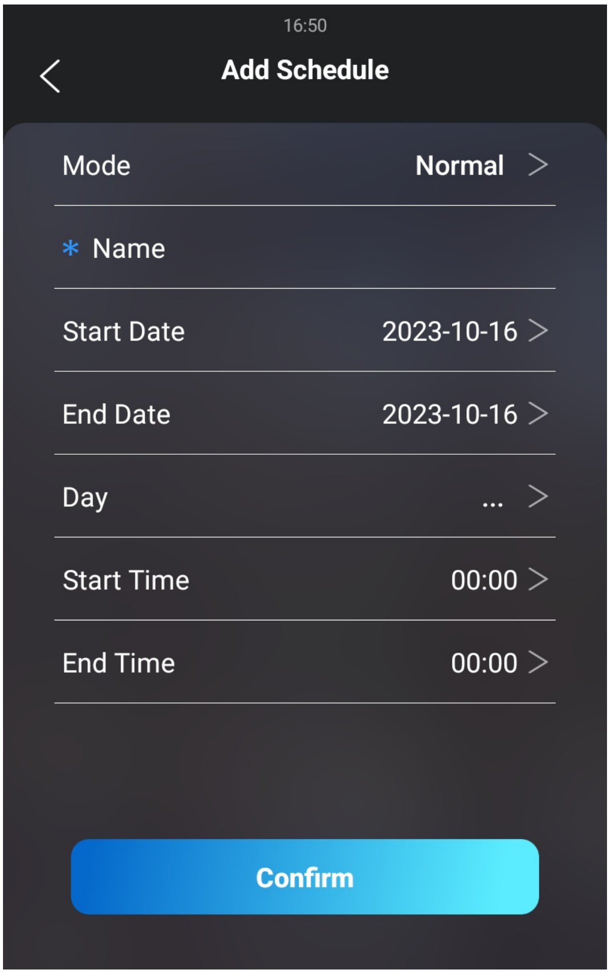
Start Date - End Date: Start Date ~ End Date

Day: ☑ Mon ☑ Tue ☑ Wed ☑ Thur ☑ Fri ☑ Sat ☑ Sun □ Check All

Start Time - End Time: 00:00 - 00:00

Create Access Schedule on the Device

Path: **Basic Setting > Schedule > Add**.



16:50

Add Schedule

Mode: Normal

* Name

Start Date: 2023-10-16

End Date: 2023-10-16

Day: ...

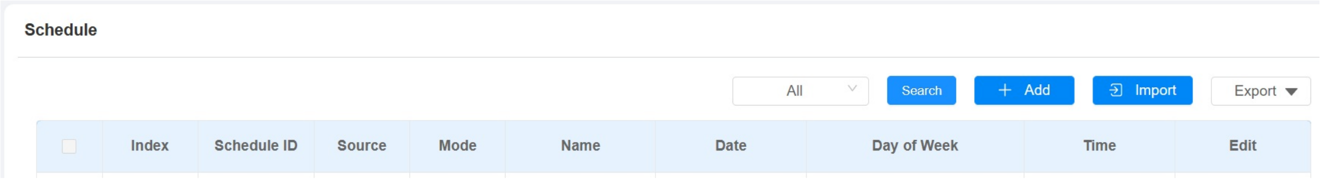
Start Time: 00:00

End Time: 00:00

Import and Export Access Schedule

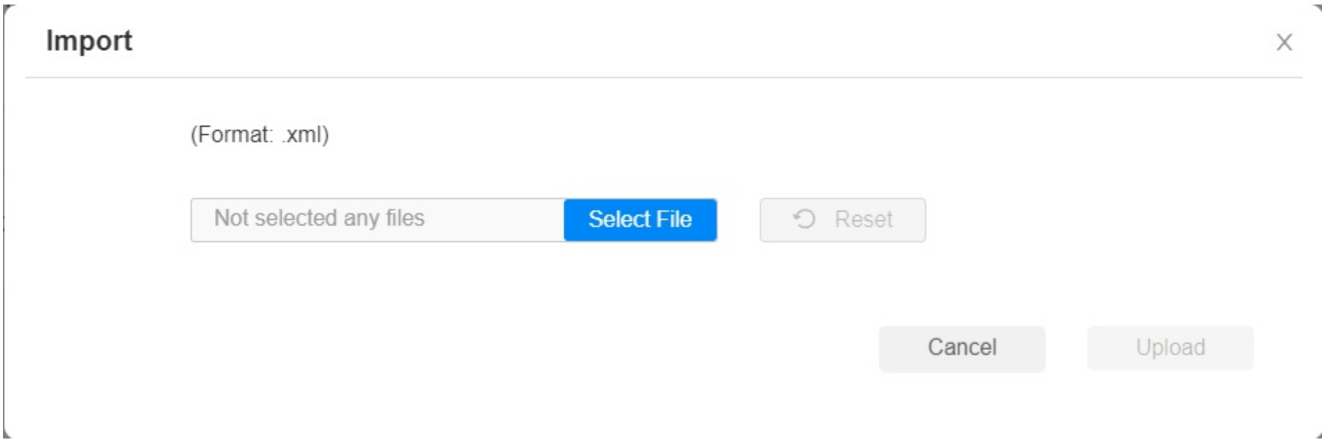
You can create door access schedules one by one or in bulk. You can export the current schedule file, edit it or add more schedules following the format, and import the new file to the desired devices. This helps you manage your door access schedules easily.

To configure it on the web **Setting > Schedule** interface.



Schedule

□	Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	Edit



Import

(Format: .xml)

Not selected any files | Select File | Reset

Cancel | Upload

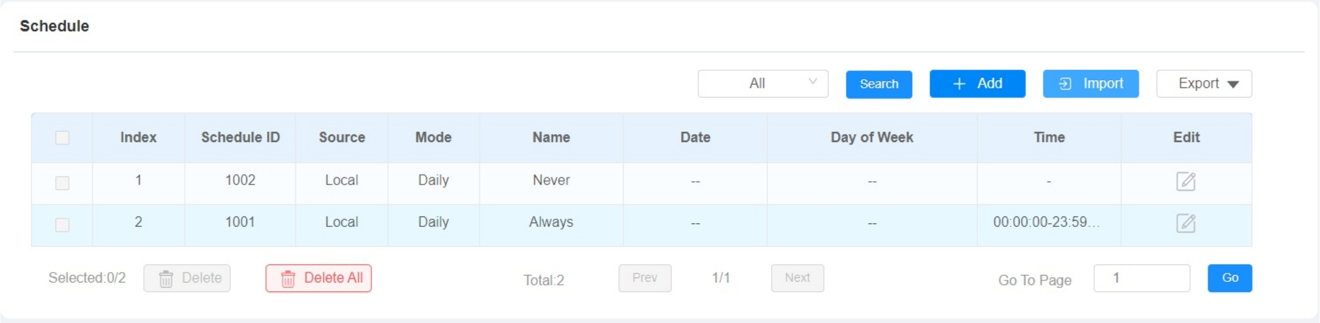
Note

- It only supports a .xml format file for importing and exporting the schedule.

Edit the Door Access Schedule

Edit the Door Access Schedule on the Web Interface

If you want to edit or delete the door access schedule you created, you can edit or delete the configured schedule separately or in batch on the web **Setting > Schedule** interface.



Schedule

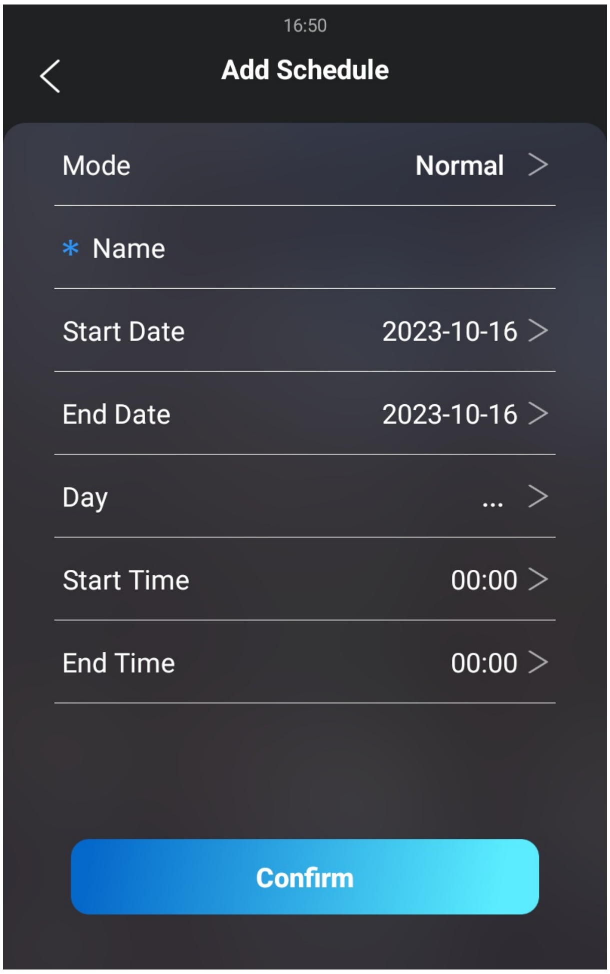
All | Search | + Add | Import | Export

□	Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	Edit
□	1	1002	Local	Daily	Never	--	--	-	✎
□	2	1001	Local	Daily	Always	--	--	00:00:00-23:59...	✎

Selected:0/2 | Delete | Delete All | Total:2 | Prev | 1/1 | Next | Go To Page 1 | Go

Edit the Door Access Schedule on the Device

Path: **Basic Setting > Schedule > Add**.



16:50

Add Schedule

Mode Normal

* Name

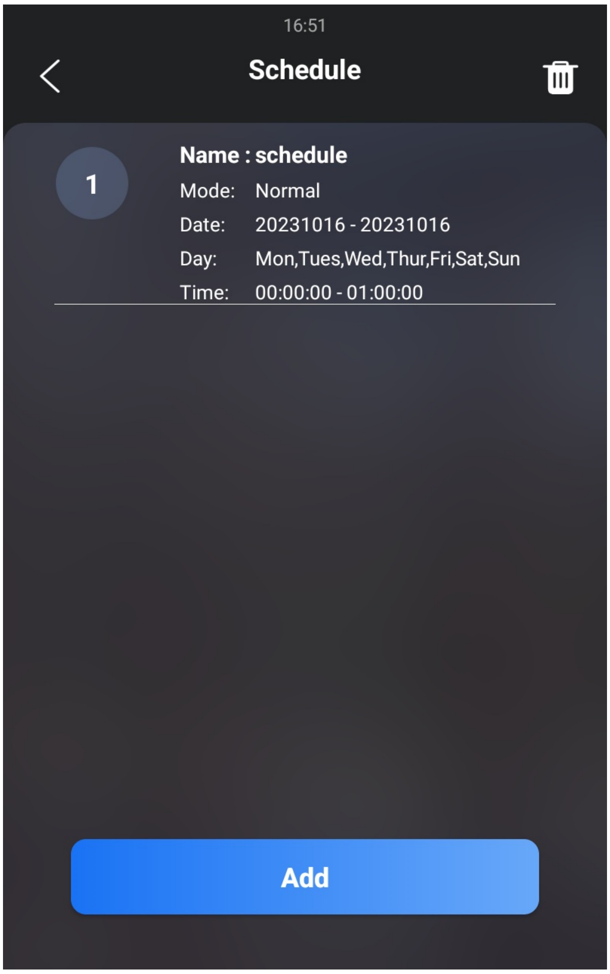
Start Date 2023-10-16

End Date 2023-10-16

Day ...

Start Time 00:00

End Time 00:00



16:51

Schedule

1

Name : schedule

Mode: Normal

Date: 20231016 - 20231016

Day: Mon,Tues,Wed,Thur,Fri,Sat,Sun

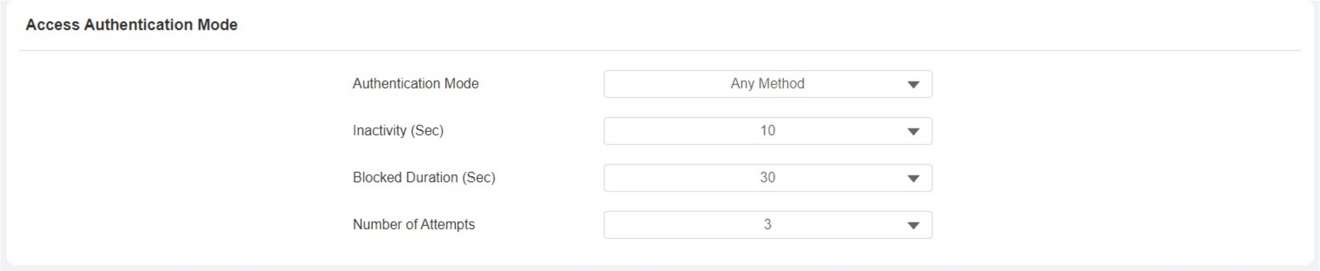
Time: 00:00:00 - 01:00:00

Door Unlock Configuration

Access Authentication

You can set up multiple access authentication modes, and set up authentication security as needed.

On the web, navigate to **Settings> Key/Display > Access Authentication Mode** interface.



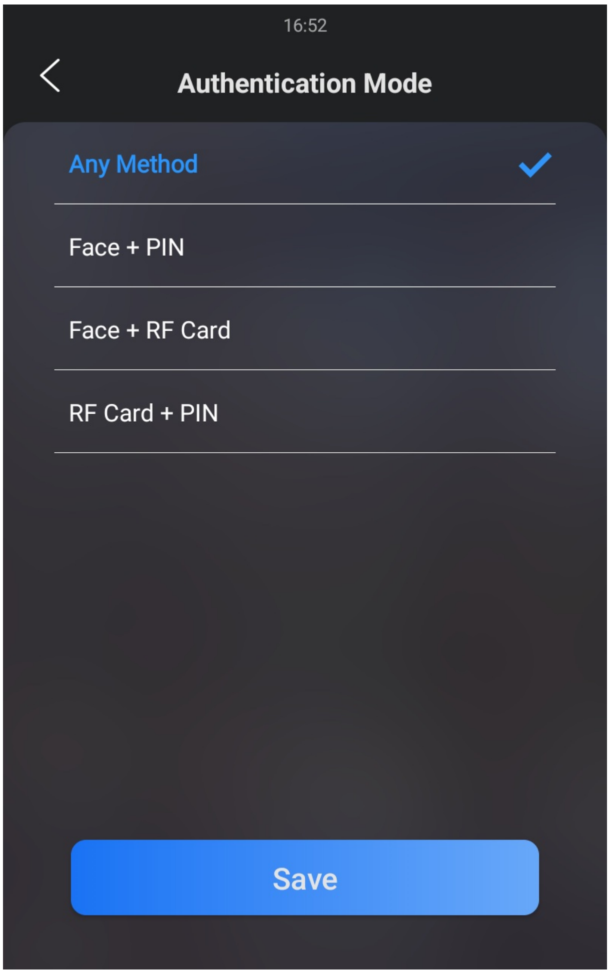
Access Authentication Mode

Authentication Mode	Any Method
Inactivity (Sec)	10
Blocked Duration (Sec)	30
Number of Attempts	3

Parameter Set-up:

- **Authentication Mode**: select **Any method** if you allow all the access methods to unlock the door. Select **Face + PIN** if you want to apply dual access methods (Face + PIN) for the door unlock. Select **Face + Card** if you want to apply dual access methods (Face+ RF Card) for the door unlock. Select **Card + PIN** if you want to apply dual access methods (Card+ PIN) for the door unlock.
- **Inactivity (Sec)**: set the authentication timeout for the second authentication. For example, in **Face+PIN** authentication, if you set the authentication timeout as 10 seconds, then you have to enter the PIN code ten seconds after you passed the face recognition, otherwise, the screen will return to the home screen.
- **Blocked Duration (Sec)**: set the block time for the first authentication. For example, if you set the number of attempts as 3, and you failed to pass the second authentication three times, then you will be temporarily blocked from the first authentication according to the block time you defined.
- **Number of Attempts**: send the number of attempts you are allowed for the second authentication.

To set up authentication mode on the device, go to **Security > Authentication Mode**.

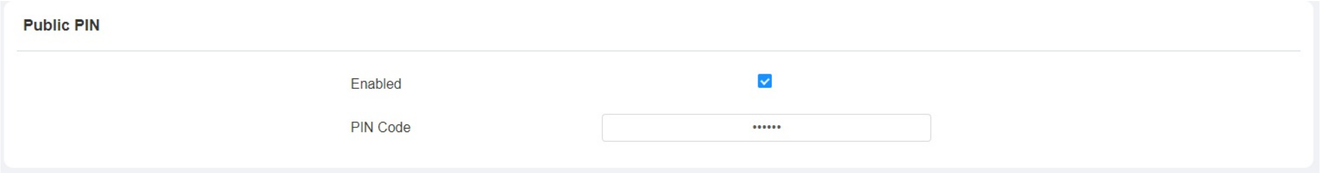


Configure PIN Code for Door Unlock

There are two types of PIN codes for door access: public and private. A private PIN is unique to each user, while the public one is shared by residents in the same building or complex. You can create and modify both the public and private PIN codes.

Configure Public PIN code

You can configure the public PIN code on the device web **Access Control** > **PIN Setting** > **Public PIN** interface.



Public PIN

Enabled ☑

PIN Code ••••••

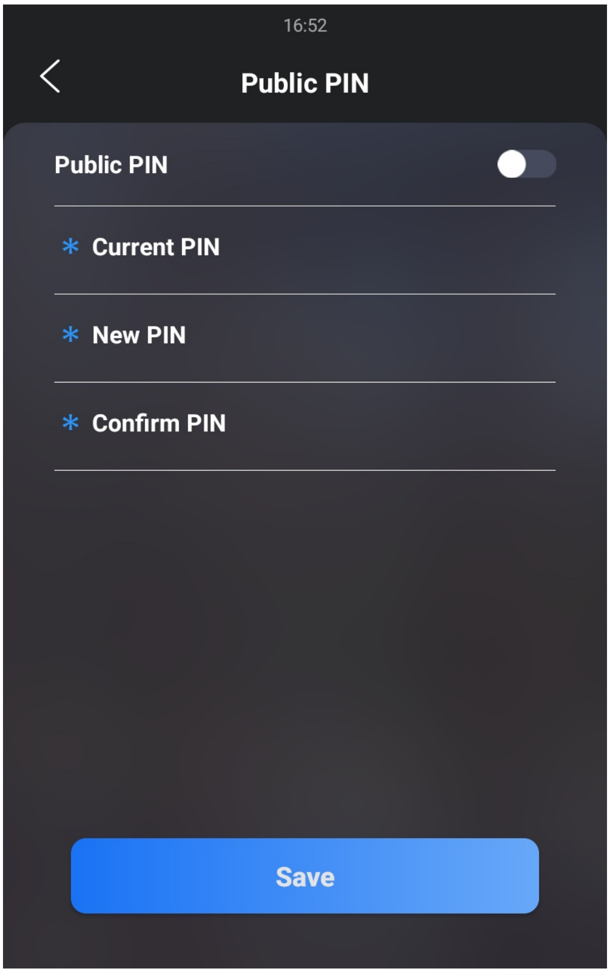
Note

- The public PIN code will not be valid until the function is turned on.

Parameter Set-up:

- **PIN Code**: set the PIN code with a digit limit ranging from 4-8.

To configure it on the device, go to **Security** > **Public PIN**.



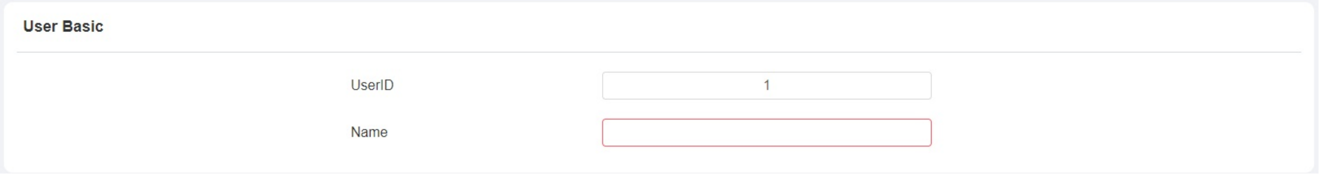
Note

- The public PIN code will not be valid until the function is turned on.

Add User

You need to create a user before you can set up a private PIN, RF card, and face data for the user. Also, you can set up access control settings and related call settings for the user.

Go to **Directory** > **User** > **+ Add** > **User Basic** interface.



User Basic

UserID	1
Name	

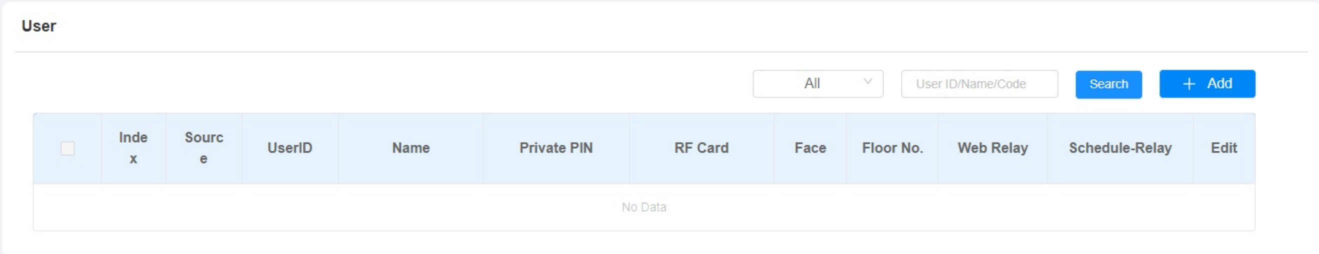
Parameter Set-up:

- **User ID**: User ID can be generated by the system automatically.

Configure Private PIN Code on the Web Interface

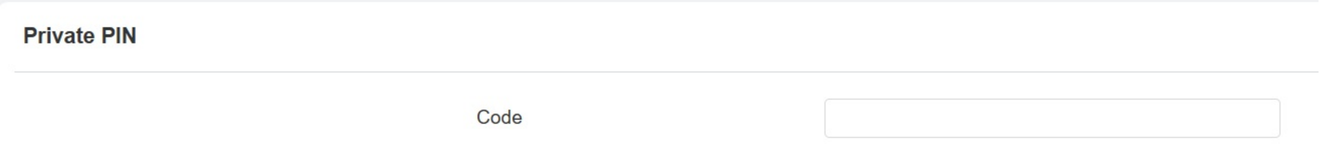
On the web interface, you can create the PIN code and customize additional settings, such as defining the door access schedule to determine when the code is valid and specifying which relay to open.

To configure on the web **Directory** > **User** > **+Add** interface.



User

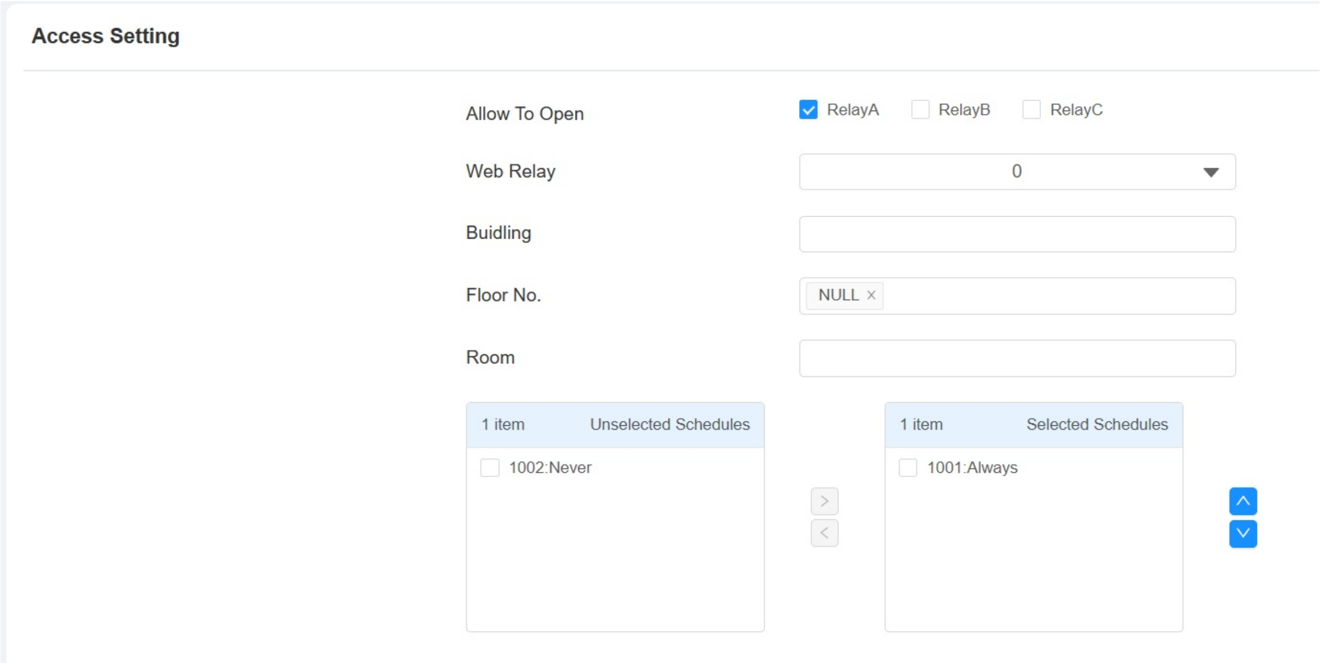
□	Index	Source	UserID	Name	Private PIN	RF Card	Face	Floor No.	Web Relay	Schedule-Relay	Edit
No Data											



Private PIN

Code	

Scroll down to Access Setting and select door access schedule for private PIN code door access:



Access Setting

Allow To Open ☑ RelayA □ RelayB □ RelayC

Web Relay 0

Buidling

Floor No. NULL ×

Room

Parameter Set-up:

- **Allow To Open**: select the relay for the door unlock for the user.
- **Web Relay**: select the specific number of web relay action commands you have set up on the web interface.
- **Schedule**: select from the created door access schedule on the left box and move the one to be applied to the user(s)-specific PIN code door access to the box on the right side.

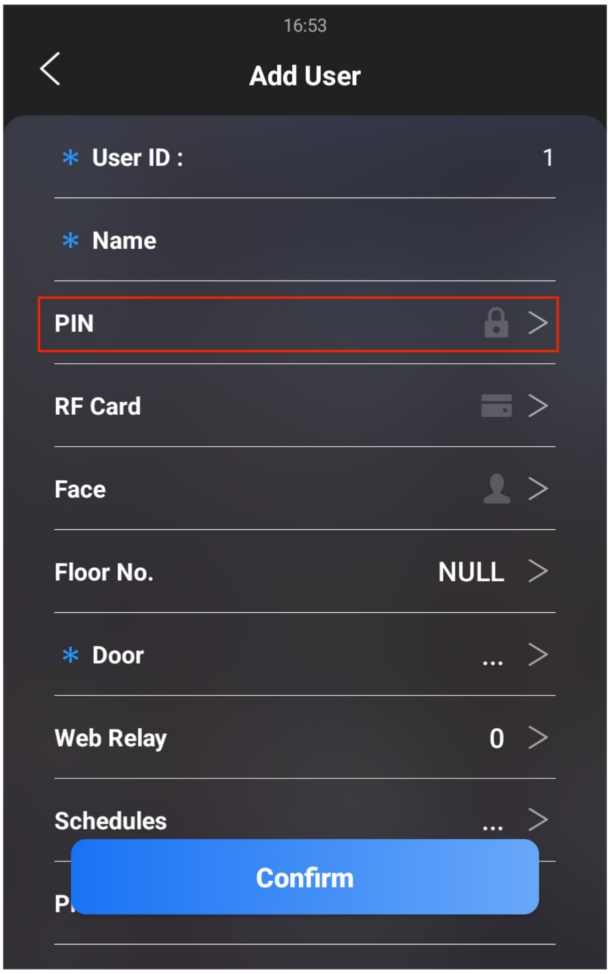
Note

- This step is applicable to door access by RF card and Facial recognition as they are identical in configuration.

Configure Private PIN Code on the Device

You can set up a private PIN code on the device for the specific user.

To configure the language display on the device **Basic Setting > User > User List >Add** screen.

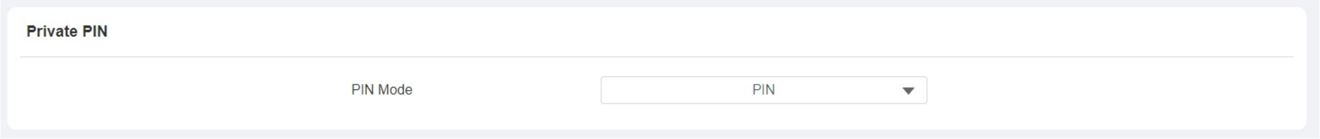

16:53

Add User

Configure Private PIN Access Mode

The device provides two authentication methods for private PIN code access: PIN and APT# + PIN. The latter requires users to input their apartment number followed by their private PIN to unlock the door.

To configure it, go to **Access Control > PIN Setting > Private PIN** interface.


Private PIN

PIN Mode: PIN

Parameter Set-up:

- **PIN Mode**: select access mode between **PIN** and **APT#+PIN.** if you select PIN then you are only required to enter the **PIN** code directly for the door access, while if you select **APT#+PIN**, then you are required to enter the Apartment Number first before entering your PIN code for the door access.

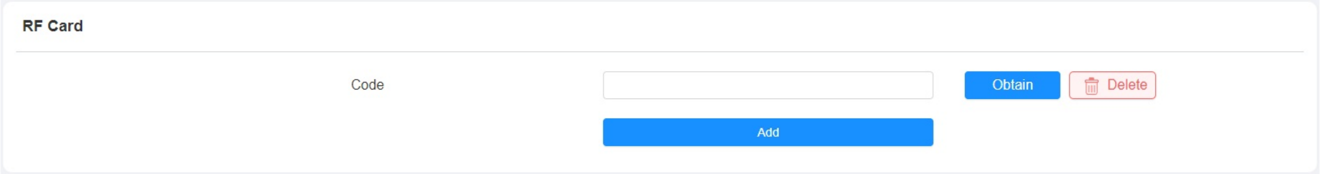
Note

- **Apartment Number** can only be applicable when the device is added to the Akuvox SmartPlus.

Configure RF Card for Door Unlock

Configure RF Card on the Web Interface

To configure it on the web **Directory > User > + Add > RF Card** interface.



RF Card

Code

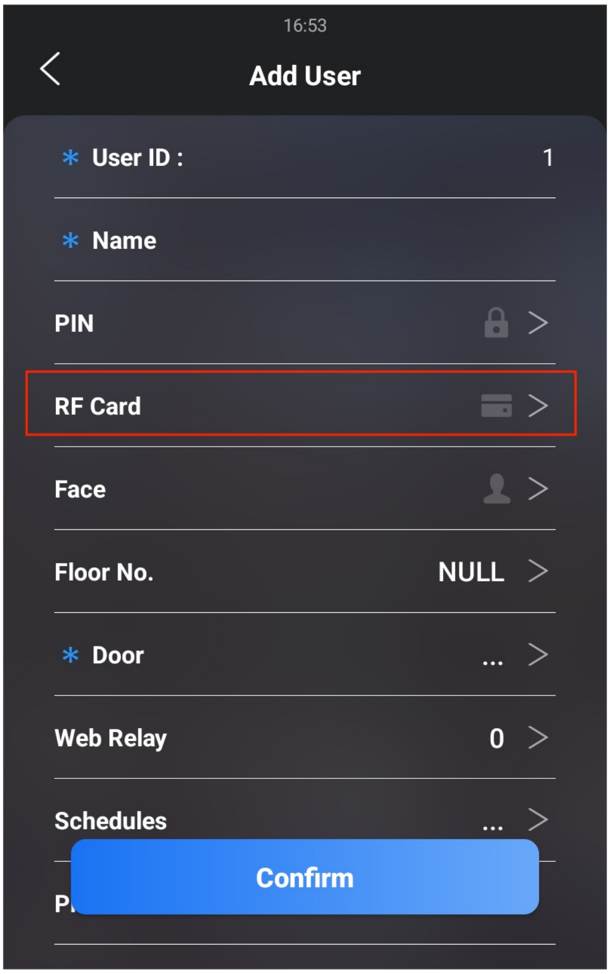
Note

- Please refer to PIN code access schedule selection for the RF card user(s)- specific door access.
- RF card with 13.56 MHz and 125 kHz can be applicable to the door phone for door access.

Configure RF Card on the device

You can configure the RF card directly on the device for the door access while setting up the time schedule for the validity of the RF card access along with the web relay that can be triggered with the RF card etc.

To configure on the device **Setting>User>User List>Add** interface.



16:53

Add User

* User ID : 1

* Name

PIN

RF Card

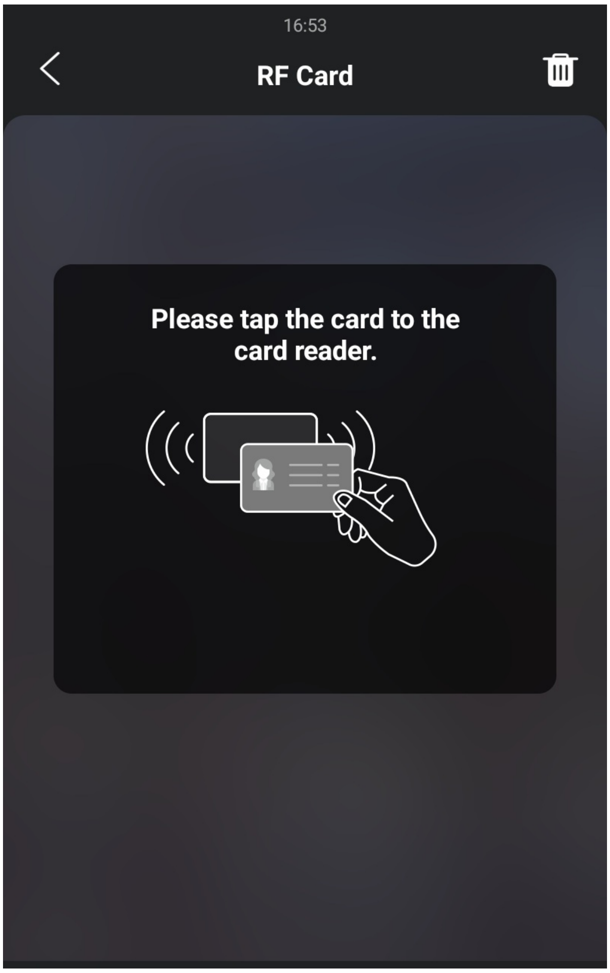
Face

Floor No. NULL

* Door ...

Web Relay 0

Schedules ...

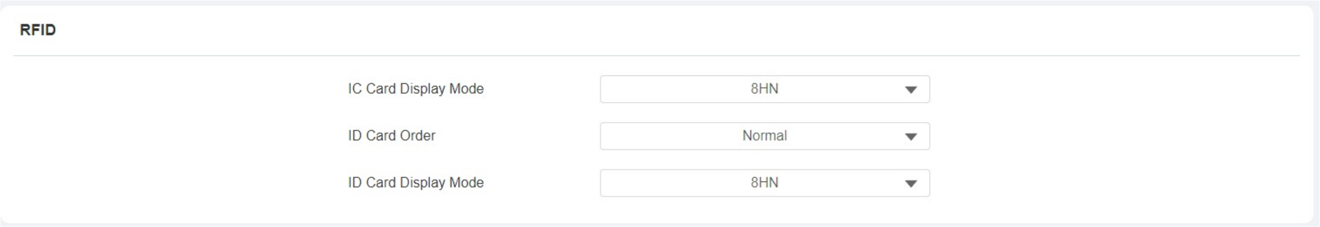


Please tap the card to the card reader.

Configure RF Card Code Format

To integrate the RF card door access with the third-party intercom system, you need to match the RF card code format with the one used by the third-party system.

To configure it, go to **Access Control** > **Card Setting** > **RFID** interface.



RFID

IC Card Display Mode	8HN
ID Card Order	Normal
ID Card Display Mode	8HN

Parameter Set-up:

- **IC-Card Display Mode**: select the card format for the ID Card for the door access (**8H10D**, **6H3D5D(W26)**, **6H8D**, **8HN**, **6H3D5D-R(W26)**, **8HR10D** and **8HR**). The card code format is 8HN by default.
- **ID Card Order**: select ID card reading in normal order or reversed order. You might need

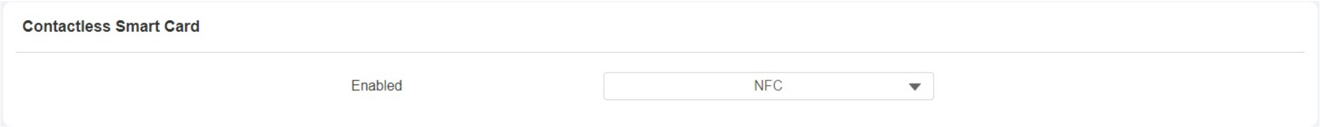
to select card orders for third-party integration (eg. third-party access control). and you can also reverse the card number for card protection.

- **ID Card Display Mode**: Select the card format for the ID Card for the door access: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR, 6H3D5D-R(W26)**, and **8HR10D**. The card code format is 8HN by default in the door phone.

Contactless Smart Card

You can select an NFC card or Felica card for contactless access. For example, if you enable both NFC and Felica cards, you can gain contactless entry with the two types of cards.

Path: **Access Control > Card Setting >Contactless Smart Card.**



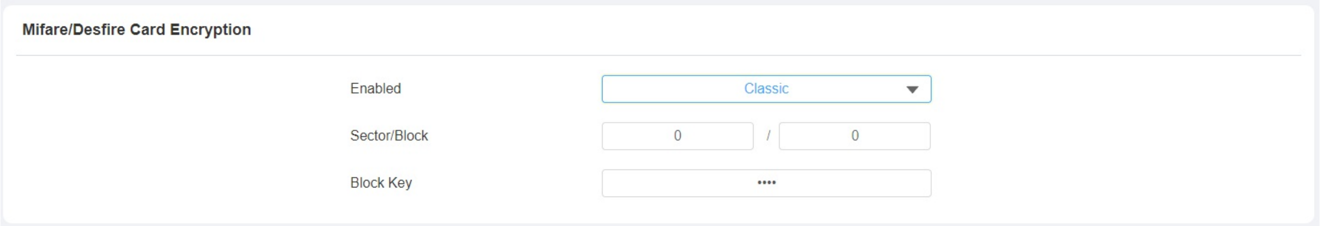
Contactless Smart Card

Enabled: NFC

Mifare/Desfire Card Encryption

The door phone can encrypt Mifare cards for greater security. When this feature is enabled, it reads the data in the cards' designated sectors and blocks, not the UID.

To do so, you can navigate to **Access Control > Card Setting > Mifare/Desfire Card Encryption.**

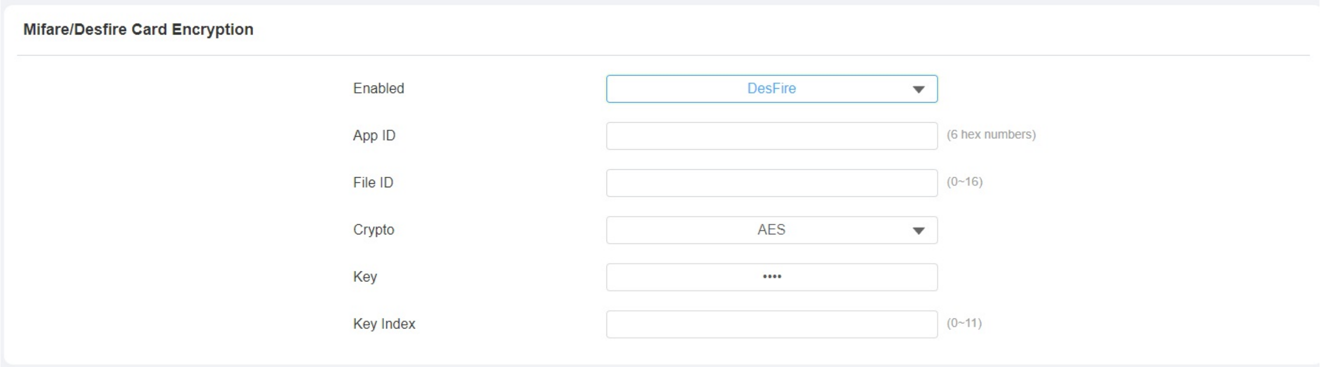


Mifare/Desfire Card Encryption

Enabled: Classic

Sector/Block: 0 / 0

Block Key: ••••



Mifare/Desfire Card Encryption

Enabled: DesFire

App ID: (6 hex numbers)

File ID: (0~16)

Crypto: AES

Key: ••••

Key Index: (0~11)

Parameter Set-up:

- **Sector/Block**: enter the sector and block in which the card number is located in the Mifare/ Defire Card. For example, the card number can be in sector 3 and block 3 in the card.
- **Block Key**: enter the block password for access.
- **Crypto**: choose from AES and DES.

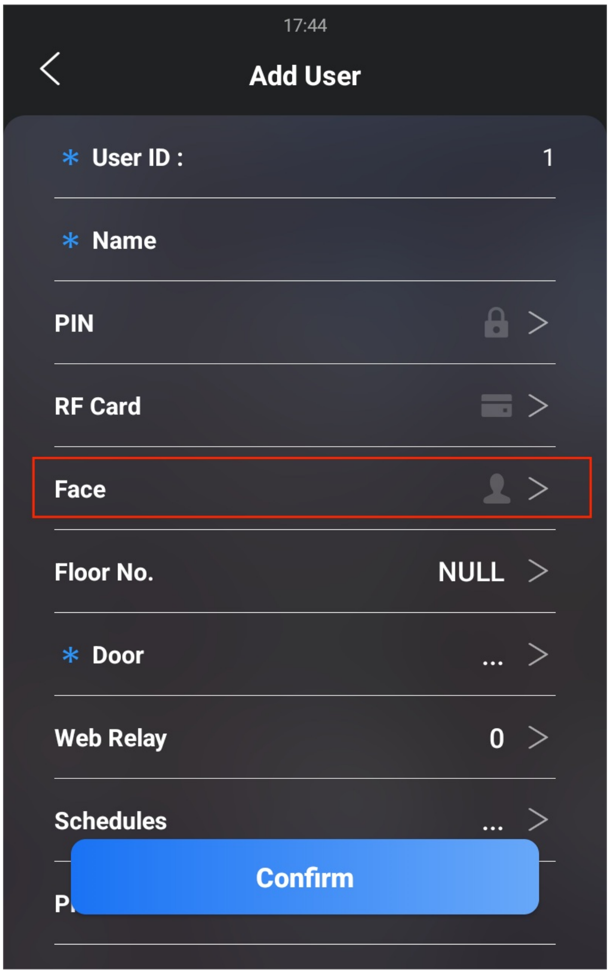
Configure Facial Recognition for Door Unlock

The door phone allows you to adjust facial recognition accuracy, recognition intervals, and more to enhance user experience.

Enroll Face Data on the Device

You can enroll face data on the device by entering the user's name and registering your facial ID on the device for door access.

To do it on the device, go to **Setting** > **User** > **User List** > **Add** > **Face** interface.



* User ID : 1

* Name

PIN

RF Card

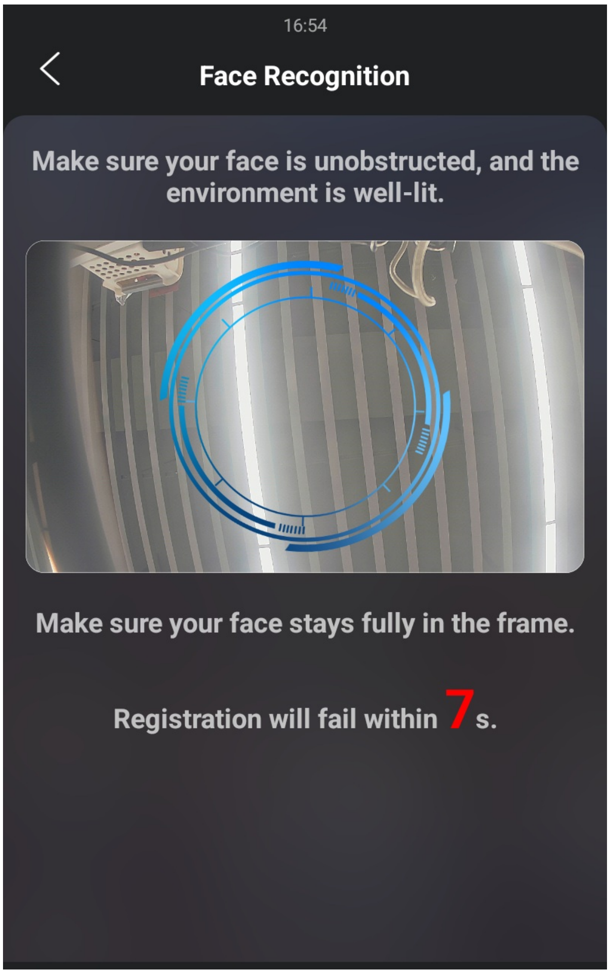
Face

Floor No. NULL

* Door ...

Web Relay 0

Schedules ...



16:54

Face Recognition

Make sure your face is unobstructed, and the environment is well-lit.

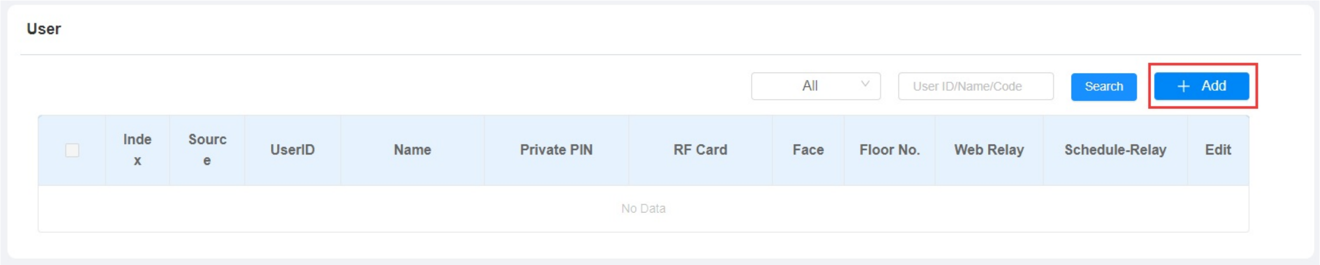
Make sure your face stays fully in the frame.

Registration will fail within 7 s.

Upload Face Data on the Web Interface

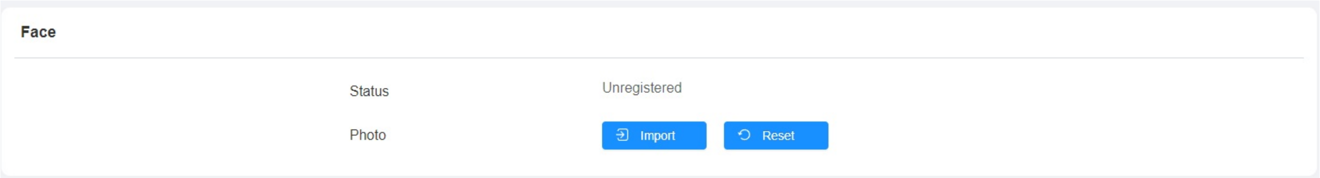
You can upload the face data to the device on the web interface.

To do so, go to **Directory > User**, then click **+Add.** After that, you can upload the face photo.



User

□	Index	Source	UserID	Name	Private PIN	RF Card	Face	Floor No.	Web Relay	Schedule-Relay	Edit
No Data											



Face

Status: Unregistered

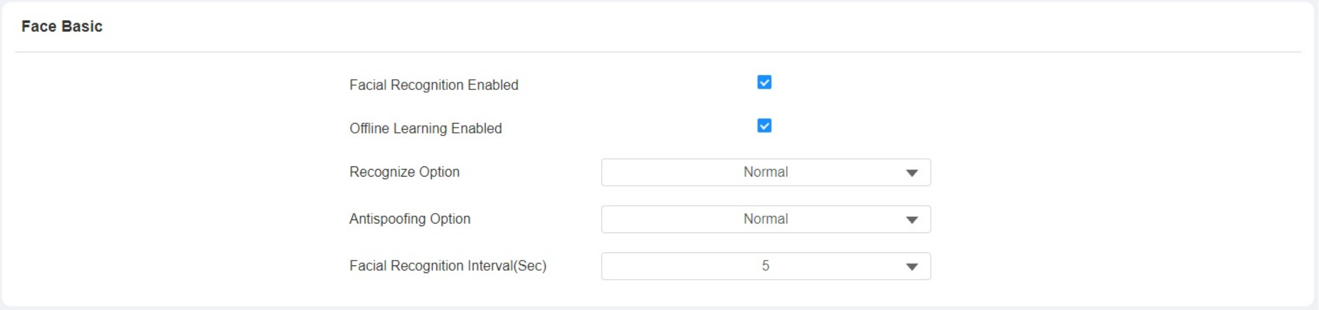
Photo

Note

- Pictures to be uploaded should be in jpg or png format.

Configure Facial Recognition on Web Interface

To configure it, go to **Access Control > Face Setting** interface.



Face Basic

Facial Recognition Enabled ☑

Offline Learning Enabled ☑

Recognize Option: Normal

Antispoofing Option: Normal

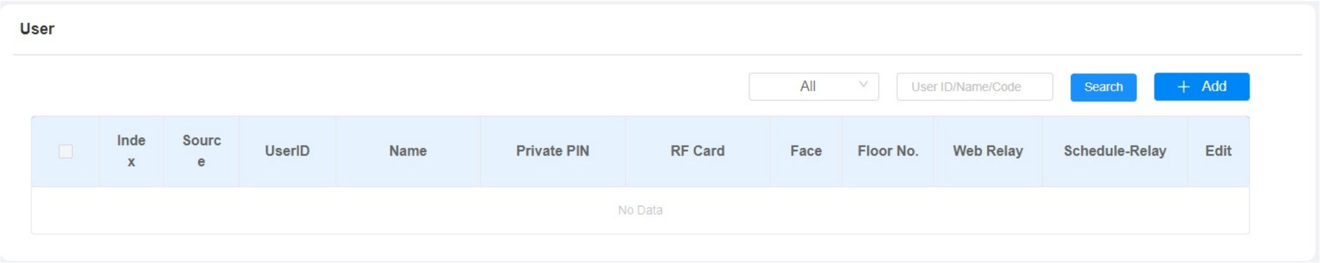
Facial Recognition Interval(Sec): 5

Parameter Set-up:

- **Offline Learning Enabled**: tick the box if you want to improve the device recognizing capability, focusing on the major facial characteristics while sidelining the minor changes that occurred to your face. Facial recognition accuracy improves as the number of facial recognition increases.
- **Recognize Option**: click to select the facial recognition accuracy level among four options: **Low, Normal, High**, and **Highest**. For example, if you select Highest then there will be the least possibility that someone else will be mistaken for you by mistake or another way around in facial recognition.
- **Antispoofing Option**: select the Anti-spoofing level among four options: **Low, Normal, High**, and **Highest**. For example, if you select **Highest** then there will be the least possibility that the device will be fooled by digital images or pictures of any kind.
- **Facial Recognition Interval(Sec)**: select a time interval between every two facial recognitions from 1-8 minutes. For example, if you select **5**, then you have to wait for 5 minutes before you are allowed to perform facial recognition again.

Edit the User-specific door Access Data

You can search user(s)-specific door access and edit the door access data on the web **Directory > User** interface.



User

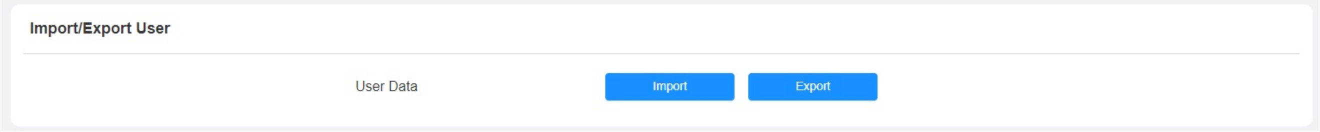
All | User ID/Name/Code | Search | + Add

□	Index	Source	UserID	Name	Private PIN	RF Card	Face	Floor No.	Web Relay	Schedule-Relay	Edit
No Data											

Import and Export User Data of Access Control

The door phone supports User Data of access control to be shared among Akuvox door phones through import and export while you can also export the facial data out of the door phone and then import it to a third-party device.

To configure it, go to **Directory>User>Import/Export User** interface.



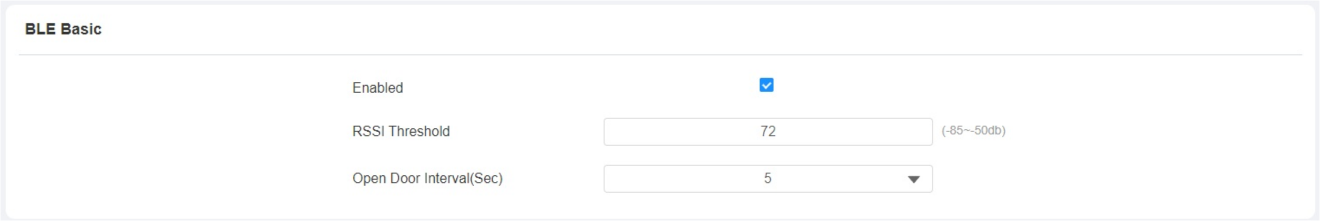
Import/Export User

User Data: Import | Export

Configure Bluetooth for Door Unlock

The Bluetooth-enabled SmartPlus app enables users to enter the door hands-free. They can either open the door with the app in their pockets or wave their phones towards the door phone as they get closer to the door.

To set up the function, navigate to **Access Control > BLE > BLE Basic.**



BLE Basic

Enabled: ☑

RSSI Threshold: 72 (-85~-50db)

Open Door Interval(Sec): 5

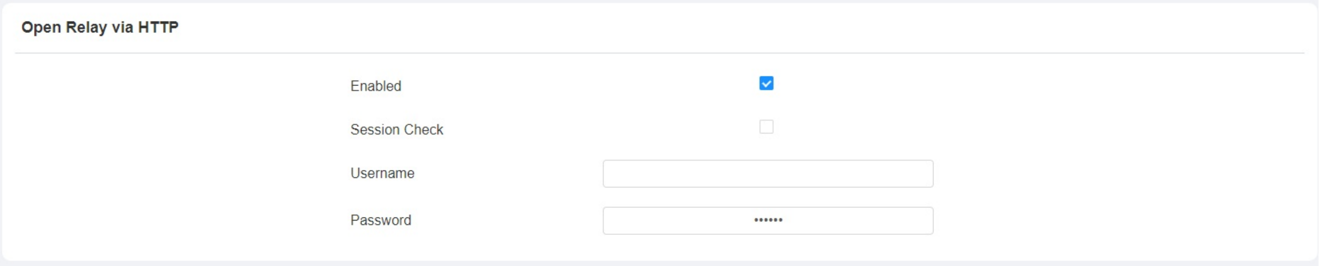
Parameter Set-up:

- **RSSI Threshold**: select the signal receiving strength from -85~-50db in absolute terms, The higher value it is, the greater strength it has. The default value is 72db in absolute terms.
- **Open Door Interval (Sec)**: select the time interval between every two Bluetooth door accesses.

Configure Open Relay via HTTP for Door Unlock

You can unlock the door remotely without approaching the device physically for door entry by typing in the created HTTP command (URL) on the web browser to trigger the relay when you are not available by the door for door entry.

To set it up, go to **Access Control** > **Relay** > **Open Relay via HTTP** interface.



Open Relay via HTTP

Enabled ☑

Session Check □

Username

Password ••••••

Parameter Set-up:

- **Session Check**: enable it to protect data transmission security.
- **User Name**: enter the user name of the device web interface, for example, **admin**.
- **Password**: enter the password for the HTTP command. For example, **12345**.

Please refer to the following example:

http://192.168.35.127/fcgi/do?
action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

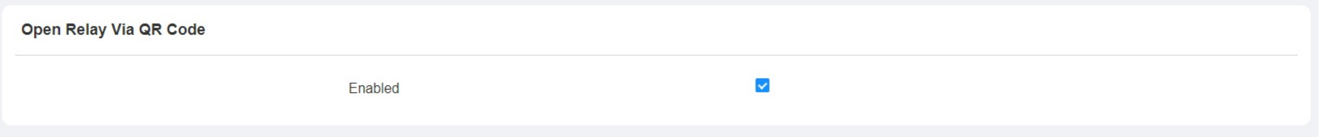
Note

- **DoorNum** in the HTTP command above refers to the relay number #1 to be triggered for the door entry.

Unlock by QR Code

You can use a QR code to unlock the door with the door phone. This method requires the Akuvox SmartPlus cloud service. You have to activate this feature before using it.

To set it up, go to **Access Control** > **Relay** > **Open Relay via QR Code** interface.



Open Relay Via QR Code

Enabled	☑

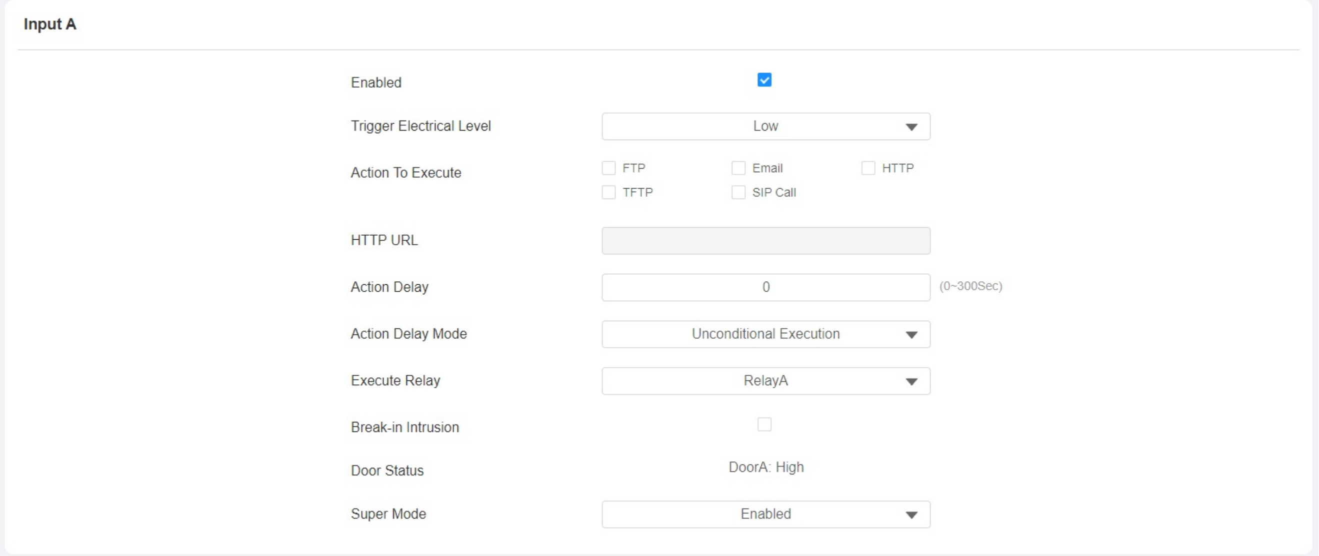
Note

- The function should work with Akuvox SmartPlus. For more information, please contact Akuvox technical support.

Configure Exit Button for Door Unlock

When users need to open the door from inside by pressing the Exit button, you need to set up the Input terminal that matches the Exit button to activate the relay for the door access.

To configure it, go to **Access Control >Input>Input A** interface.



Input A

Enabled	☑
Trigger Electrical Level	Low
Action To Execute	□ FTP □ Email □ HTTP □ TFTP □ SIP Call
HTTP URL	
Action Delay	0 (0~300Sec)
Action Delay Mode	Unconditional Execution
Execute Relay	RelayA
Break-in Intrusion	□
Door Status	DoorA: High
Super Mode	Enabled

Parameter Set-up:

- **Trigger Electrical Level**: select the trigger electrical level options between **High** and **Low** according to the actual operation of the exit button.
- **Action to Execute**: select the method to carry out the action among four options: **FTP, Email, HTTP**, and **TFTP**.
- **HTTP URL**: enter the URL if you select the HTTP to carry out the action.
- **Action Delay**: set up the delay time when the action is carried out. For example, if you set the action delay time at 5 seconds, then the corresponding actions will be carried out 5 minutes after you press the button(input is triggered).
- **Action Delay Mode**: if you select **Unconditional Execution**, then action will be carried

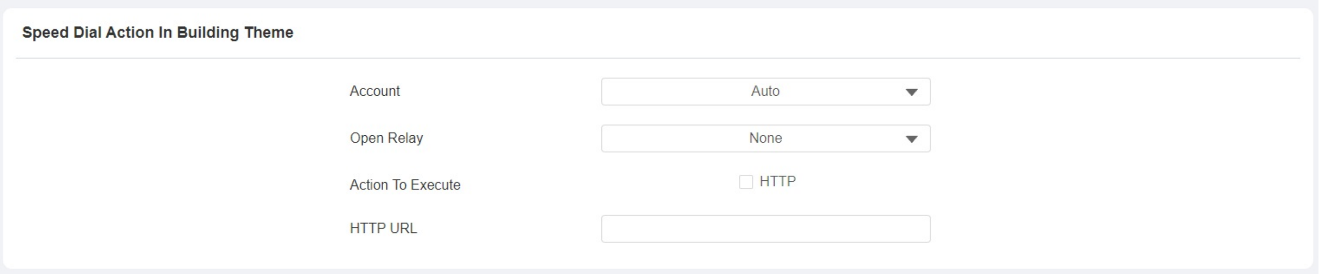
out when the input is triggered. If you select **Execute If Input Still Triggered**, then the action will be carried out if the input stays triggered. For example, if the door stays open after triggering input, an action such as an email will be sent to notify the receiver.

- **Execute Relay**: set up relays to be triggered by the input.
- **Break-in Intrusion**: enable it to trigger alarm when the door is unlocked abnormally.
- **Super Mode**: if you enable the super mode, the administrator will be able to open the door using an RF card even when the door phone breaks down or malfunctions.

Configure Reception Tab for Door Unlock

The Reception button is a tab on the home screen that allows residents and visitors to contact the receptionist or the security guard of the building. They can tap this button to ask for help or access to the door.

To configure it, go to **Setting > Key/Display > Speed Dial Action In Building Theme** interface.



Speed Dial Action In Building Theme

Account	Auto
Open Relay	None
Action To Execute	□ HTTP
HTTP URL	

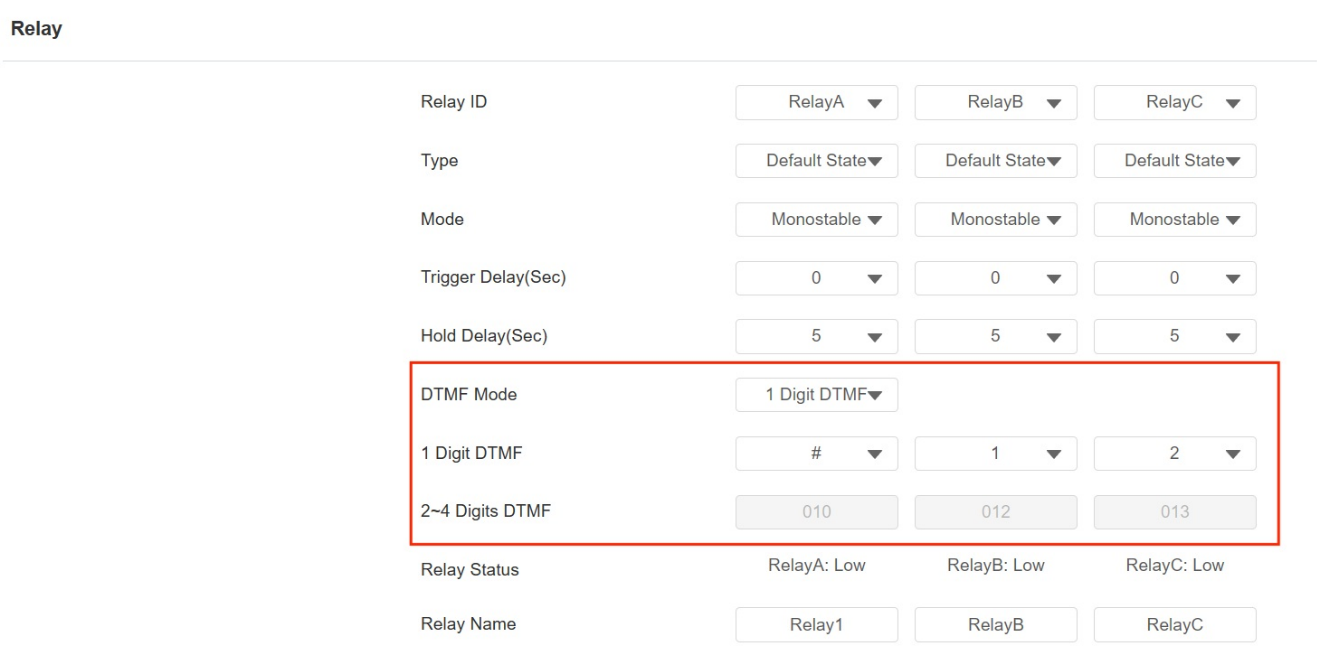
Parameter Set-up:

- **Open Relay:** select the relay(s) to be triggered by pressing the Reception Icon.
- **Action To Execute**: tick the check box to enable the HTTP option.
- **HTTP URL**: enter the URL command to be sent for door access. For example, http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

Unlock by DTMF Code

Dual-tone multi-frequency signaling(**DTMF**) is a way of sending signals over phone lines by using different voice-frequency bands. Users can use the DTMF function to unlock the door for visitors during a call by either typing the DTMF code on the soft keypad, or tapping the unlock tab with the DTMF code on the screen.

To configure it, go to **Access Control > Relay** interface.



Relay

Relay ID	RelayA	RelayB	RelayC
Type	Default State	Default State	Default State
Mode	Monostable	Monostable	Monostable
Trigger Delay(Sec)	0	0	0
Hold Delay(Sec)	5	5	5
DTMF Mode	1 Digit DTMF		
1 Digit DTMF	#	1	2
2~4 Digits DTMF	010	012	013
Relay Status	RelayA: Low	RelayB: Low	RelayC: Low
Relay Name	Relay1	RelayB	RelayC

Note

- Please refer to **Configure DTMF Data Transmission** in **Call Setting** for the specific DTMF code setting.
- Intercom devices involved must be consistent in the DTMF type otherwise DTMF code cannot be applied.

Security

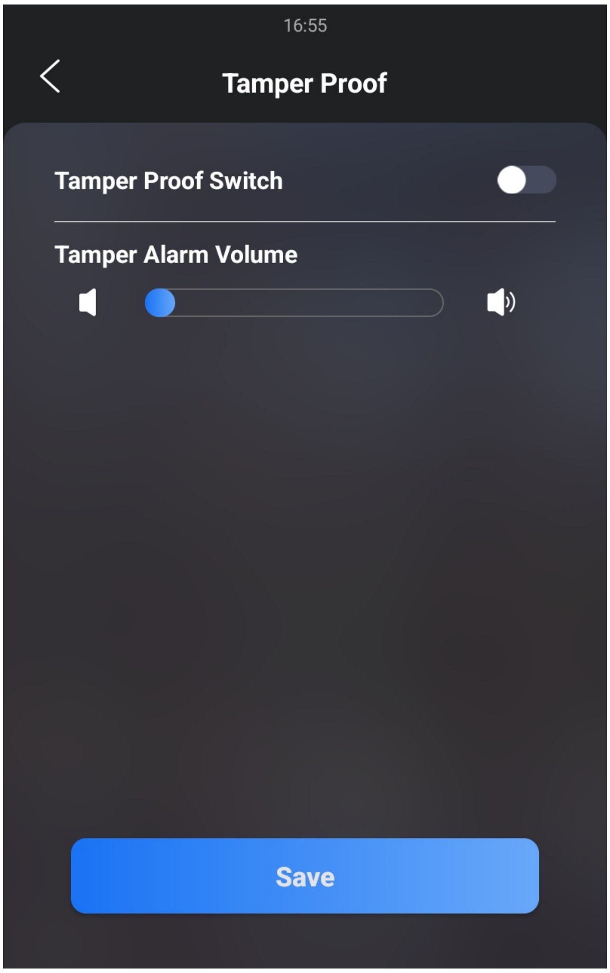
Tamper Alarm Setting

The tamper alarm function prevents anyone from removing the devices without permission. It does this by setting off the tamper alarm and making calls to a designated location when the device detects a change in its gravity value from the original one.

Configure Tamper Alarm on the Device

The tamper alarm and gravity sensor can be easily set up on the door phone.

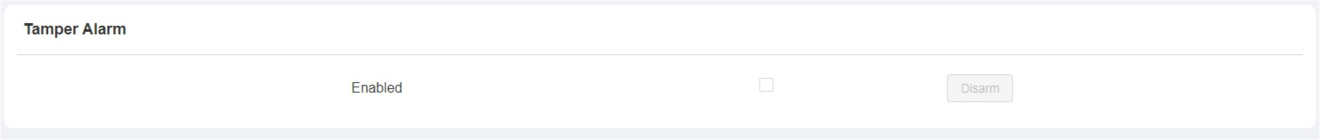
To configure the tamper alarm, go to **Setting > Security > Tamper Proof.**



Configure Tamper Alarm on the Web Interface

You can also enable the tamper alarm function on the web interface.

To configure on the web **System > Security > Tamper Alarm** interface.



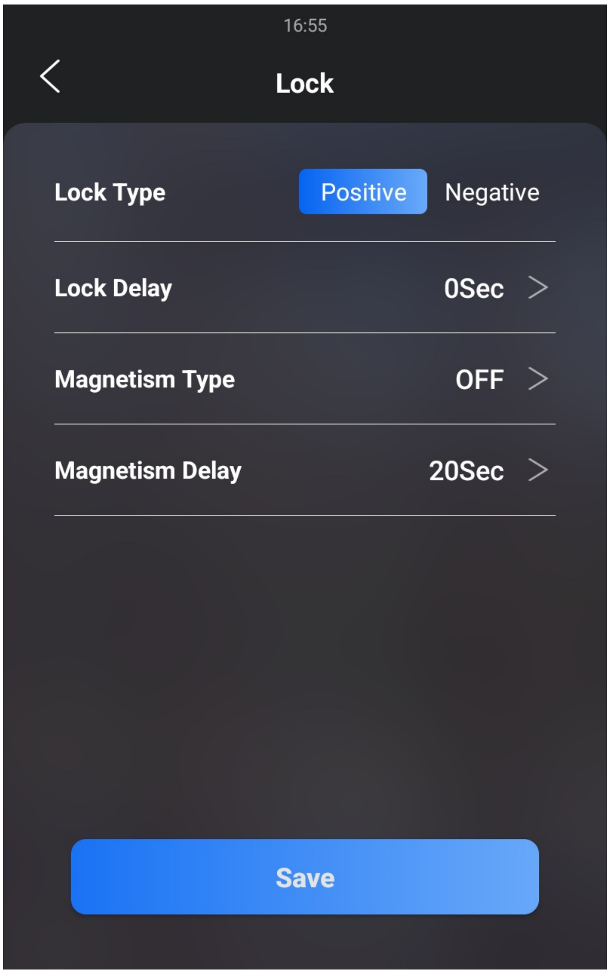
Tamper Alarm

Enabled □ Disarm

Lock Security

The door phone can work with other door locks and sensors to keep the lock secure. It will sound the alarm to alert users if the door sensor finds the door open or not fully closed.

On the device, go to **Security > Lock** for the setting.

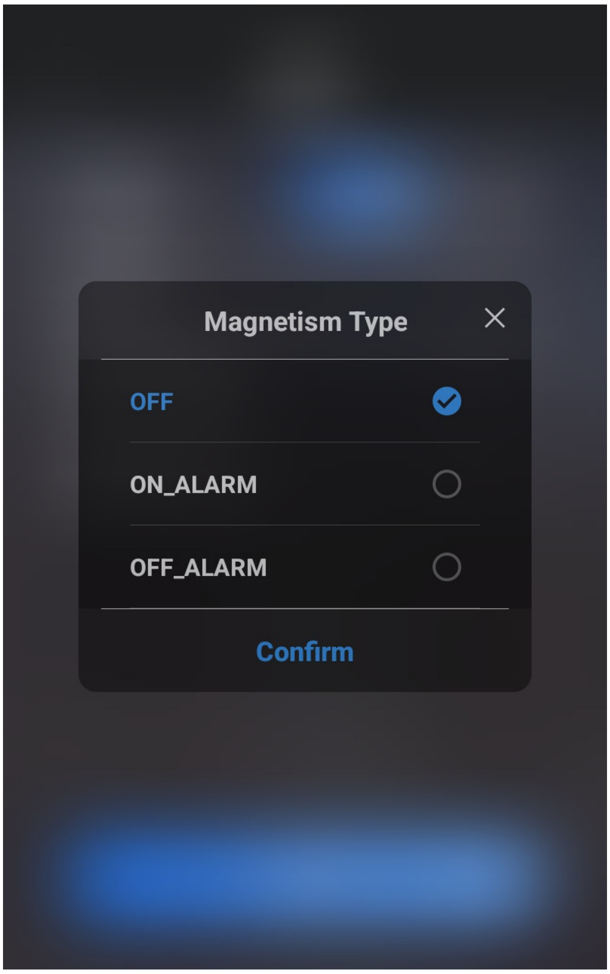


Lock Type: Positive Negative

Lock Delay: 0Sec

Magnetism Type: OFF

Magnetism Delay: 20Sec



Magnetism Type ✕

OFF ✓

ON_ALARM ○

OFF_ALARM ○

Confirm

Parameter Set-up:

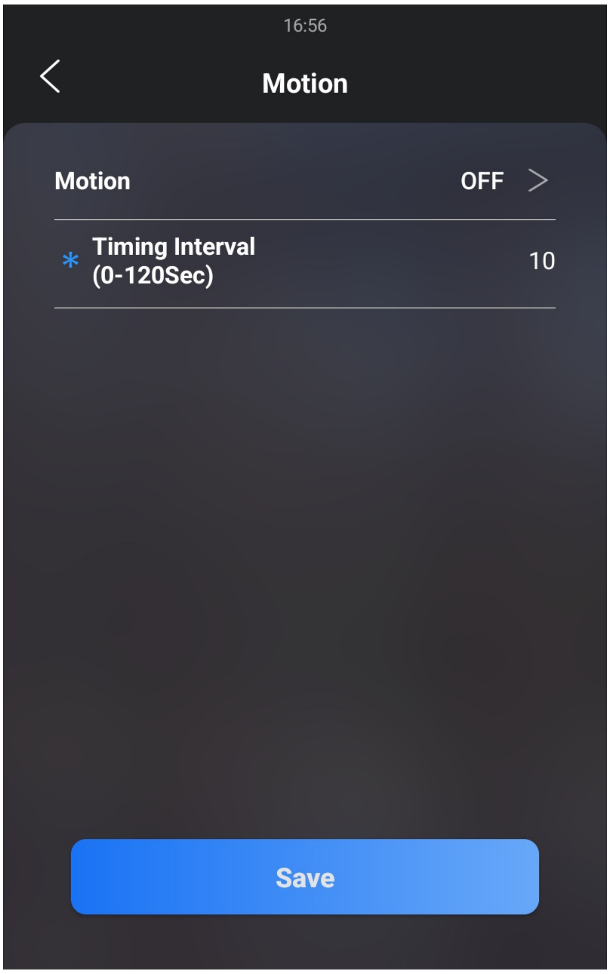
- **Lock Type**: select **Positive** for the lock that unlocks when the power is on and select **Negative** for the lock that unlocks when the power is off.
- **Lock Delay**: select door unlocks delay time after you are granted door access. The delay time range is from 0-10 seconds.
- **Magnetism Type**: select **OFF** if you want to disable the door sensor and alarm. To set the alarm trigger type, you must select **ON-ALARM** and **OFF_ALARM** according to the type of lock you applied. Select **ON_ALARM** for a positive lock, while select **OFF_ALARM** for a negative lock.
- **Magnetism Delay**: select the alarm delay time after its being triggered. The delay range is from 10-120 seconds.

Motion Detection

Motion Detection is a feature that allows unattended video surveillance and automatic alarms. It detects any changes in the image captured by the camera, such as someone walking by or the lens being moved, and activates the system to perform the appropriate action.

Configure Motion Detection on the Device

You can turn on the motion detection and set up the motion detection interval on the device **Advanced Setting** > **Surveillance** > **Motion** screen.



16:56

Motion

Motion OFF

* Timing Interval (0-120Sec) 10

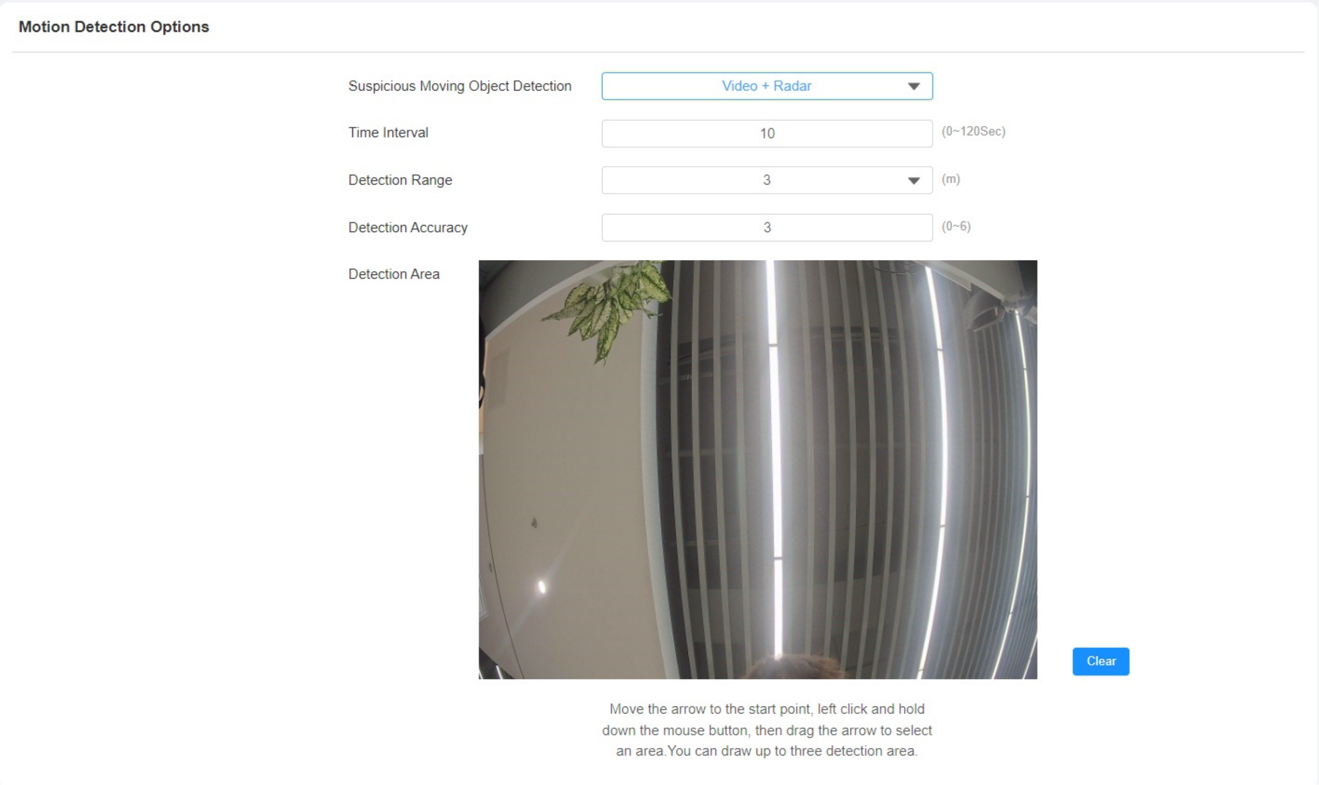
Parameter Set-up:

- **Interval**: the absolute triggering interval is 3 seconds. If you select a number greater than 3 seconds, then it requires a second triggering interval to trigger the alarm. For example, if you select 3 seconds, then the alarm will be triggered when a moving object is detected one time from 0 to 3 seconds (triggered any time from 0 to 3 seconds). However, for example, if you select 5 seconds (greater than 3), then the alarm will not be triggered until a moving object is detected for the second time from 3 to 5 seconds (triggered any time from 3 to 5 seconds). The default interval is 10 seconds.

Configure Motion Detection on the Web Interface

You can adjust various motion detection settings on the device web interface, such as the time interval, the sensitivity level, the notification method when motion is detected, and more.

To configure it on the web **Surveillance > Motion > Motion Detection Options** interface.



Motion Detection Options

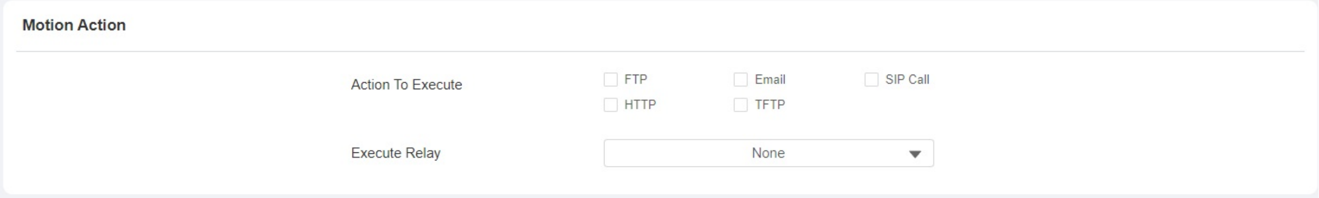
Suspicious Moving Object Detection	Video + Radar	
Time Interval	10	(0~120Sec)
Detection Range	3	(m)
Detection Accuracy	3	(0~6)
Detection Area		

Move the arrow to the start point, left click and hold down the mouse button, then drag the arrow to select an area.You can draw up to three detection area.

Parameter Set-up:

- **Suspicious Moving Object Detection**: select from **Disabled, Video Detection, Radar Detection**, and **Video + Radar.**
- **Time Interval**: set the time interval in the same way as you do on the device.
- **Detection Range**: set the radar detection range (1-3 meters). The default detection range is 3 meters.
- **Detection Accuracy**: set the detection accuracy for the detection sensitivity (0-6). The higher value, the greater sensitivity. The default detection accuracy value is 3.

After you set up the interval, you can set up the action you need.



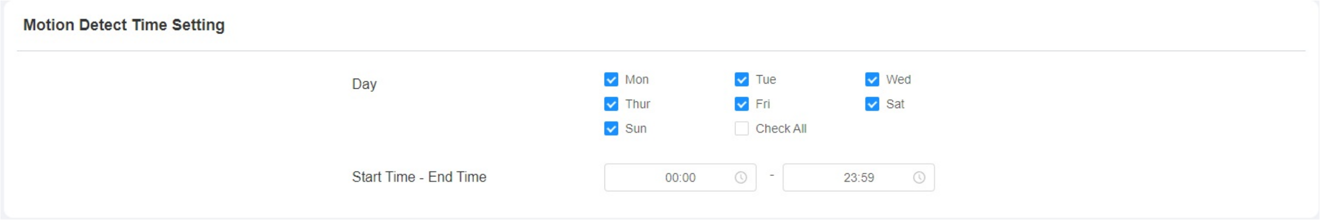
Motion Action

Action To Execute	□ FTP □ HTTP	□ Email □ TFTP	□ SIP Call
Execute Relay	None		

Parameter Set-up:

- **Action To execute**: select the method to carry out the action: FTP, Email, HTTP, TFTP, SIP Call. For example, if you select Email, then an Email will be sent to you after the motion detection alarm is triggered.
- **Action HTTP URL**: enter the HTTP command that will be sent to a third-party server to carry out the predefined action.
- **Action Relay**: select one of the door phone relays to carry the predefined action.

Scroll down and you can also set the motion detection time schedule.



Motion Detect Time Setting

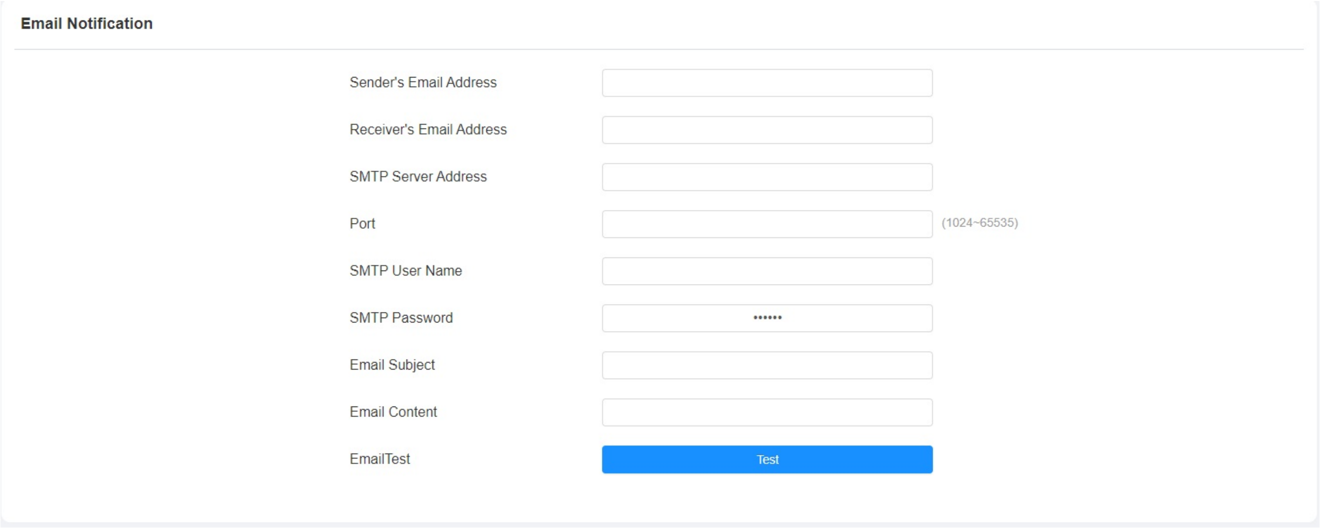
Day	☑ Mon	☑ Tue	☑ Wed
	☑ Thur	☑ Fri	☑ Sat
	☑ Sun	□ Check All	
Start Time - End Time	00:00	-	23:59

Security Notification Setting

Email Notification Setting

Set up email notification to receive screenshots of unusual motion from the door phone.

Navigate to **Setting > Action > Email Notification** interface.



Email Notification

Sender's Email Address	
Receiver's Email Address	
SMTP Server Address	
Port	(1024~65535)
SMTP User Name	
SMTP Password	••••••
Email Subject	
Email Content	
EmailTest	Test

Parameter Set-up:

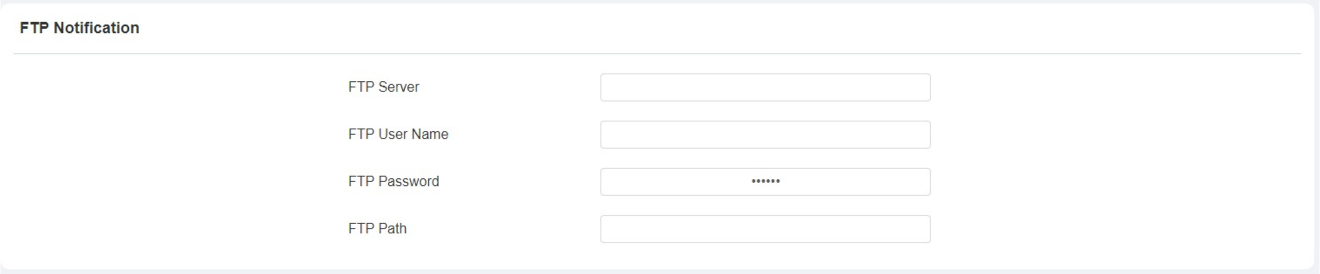
- **SMTP User Name**: enter the SMTP user name, which is usually the same as the sender’s email address.
- **SMTP Password**: configure the password of the SMTP service, which is the same as the

sender’s email address.

FTP Notification Setting

To get notifications through FTP server, you need to set up the FTP settings. The door phone will upload a screenshot to the specified FTP folder if it senses any unusual motion.

Go to **Setting** > **Action** > **FTP Notification** interface.



FTP Notification

FTP Server

FTP User Name

FTP Password ••••••

FTP Path

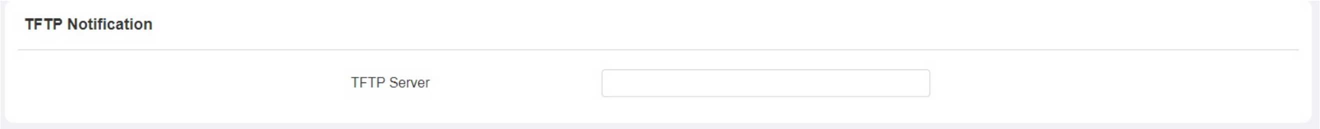
Parameter Set-up:

- **FTP Path**: enter the folder name you created in the FTP server.

TFTP Notification Setting

To receive security notifications via TFTP server, you need to enter the TFTP server address.

Go to **Setting** > **Action** > **TFTP Notification** interface.



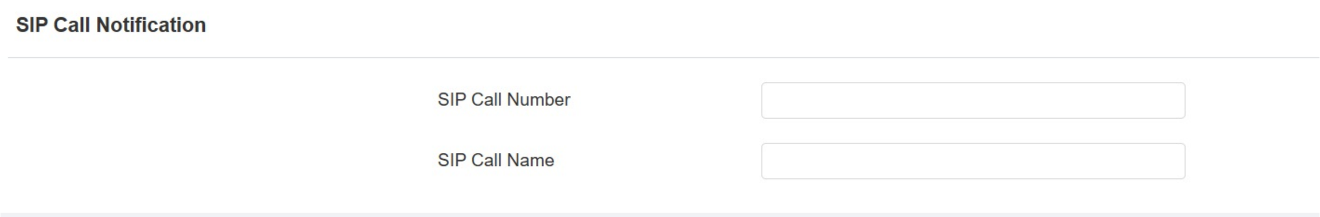
TFTP Notification

TFTP Server

SIP Call Notification

You can enter the SIP number to receive the notification.

Go to **Setting** > **Action** > **SIP Call Notification** interface.



SIP Call Notification

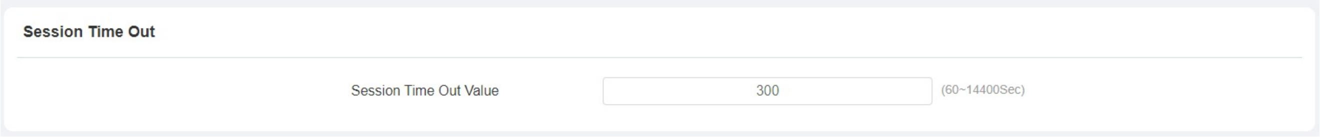
SIP Call Number

SIP Call Name

Web Interface Automatic Log-out

You can set up the web interface's automatic log-out timing, requiring re-login by entering the user name and the passwords for security purposes or for the convenience of operation.

To configure on the web **System > Security > Session Time Out** interface.



Session Time Out

Session Time Out Value: 300 (60~14400Sec)

Parameter Set-up:

- **Session Time Out Value**: set the automatic web interface log-out timing ranging from 60 seconds to 14400 seconds. The default value is 300.

Action URL

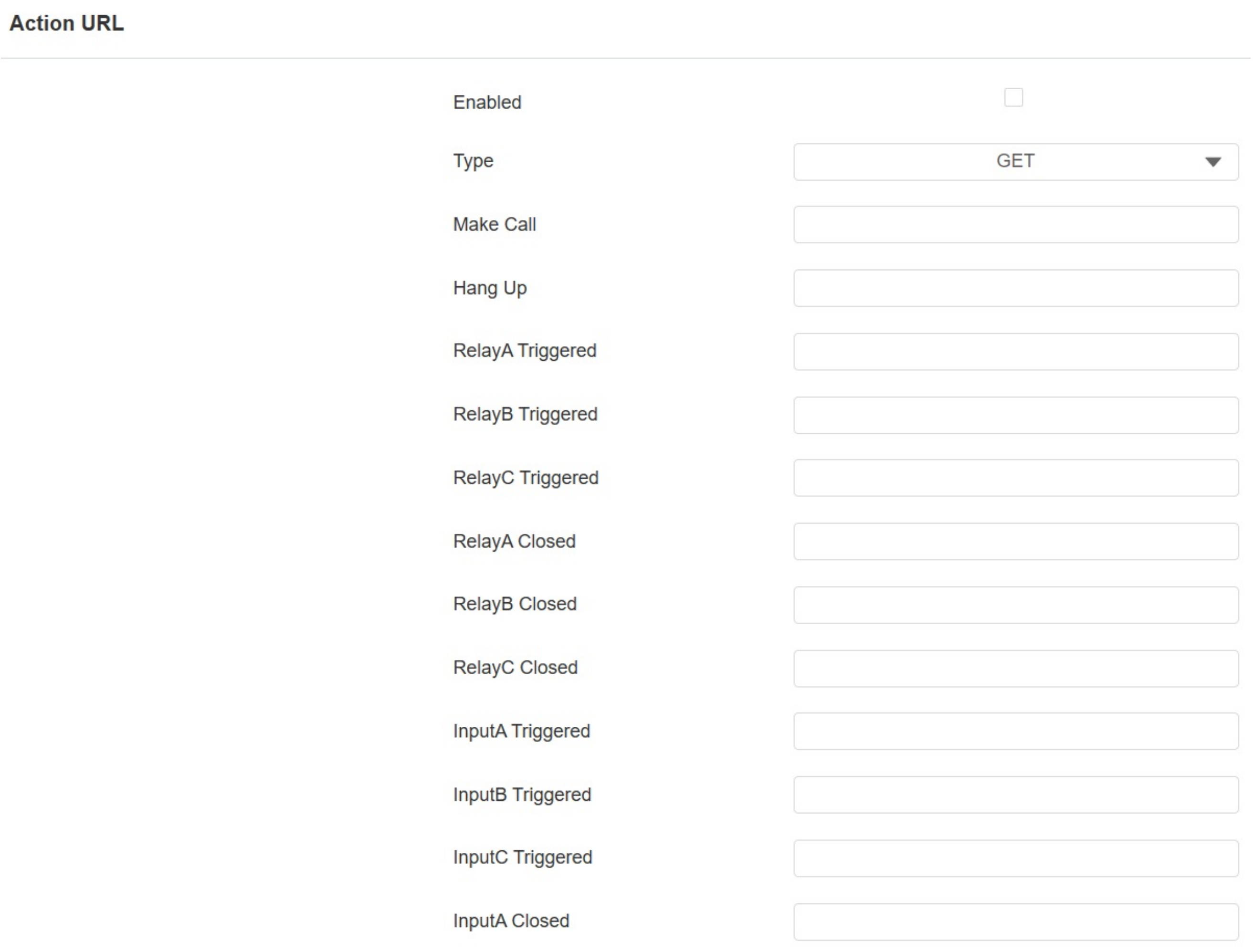
You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status, input status, PIN code, or RF card access changes.

Akuvox Action URL:

No	Event	Parameter format	Example
1	Make Call	$remote	Http://server ip/ Callnumber=$remote
2	Hang Up	$remote	Http://server ip/ Callnumber=$remote
3	Relay Triggered	$relay1status	Http://server ip/ relaytrigger=$relay1status
4	Relay Closed	$relay1status	Http://server ip/ relayclose=$relay1status
5	Input Triggered	$input1status	Http://server ip/ inputtrigger=$input1status
6	Input Closed	$input1status	Http://server ip/ inputclose=$input1status
7	Valid Code Entered	$code	Http://server ip/ validcode=$code
8	Invalid Code Entered	$code	Http://server ip/ invalidcode=$code
9	Valid Card Entered	$card_sn	Http://server ip/ validcard=$card_sn
10	Invalid Card Entered	$card_sn	Http://server ip/ invalidcard=$card_sn
11	Tamper Alarm Triggered	$alarm status	Http://server ip/tampertrigger=$alarm status

For example: http://192.168.16.118/help.xml?
mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn

You can navigate to **Settings > Actions URL.**



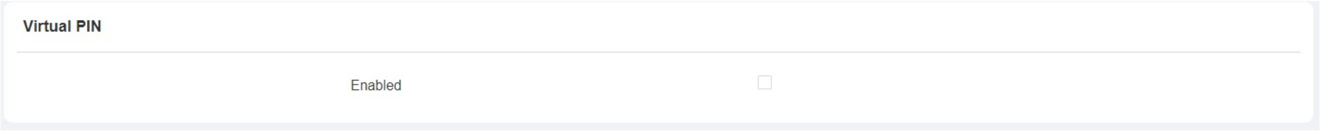
Action URL

Enabled	□
Type	GET
Make Call	
Hang Up	
RelayA Triggered	
RelayB Triggered	
RelayC Triggered	
RelayA Closed	
RelayB Closed	
RelayC Closed	
InputA Triggered	
InputB Triggered	
InputC Triggered	
InputA Closed	

Virtual PIN

The virtual PIN allows you to protect your PIN code from being leaked to someone.

To enable the virtual PIN feature, navigate to **Access Control > PIN Setting > Virtual PIN.**



Virtual PIN

Enabled	□

Parameter Set-up:

- **Enabled**: if enabled, you are allowed to put fake numbers on both ends of the PIN code for PIN code protection. For example, if your password is 1234567 you can put 99 and 88 on both ends (**99123456788**). And the virtual password is matched to the users by the number of digits that are matched. For example, if user A has a greater number of digits that are matched with the virtual password entered than user B, then it will be regarded as user A’s password. However, when double authentication is applied, then the virtual password will be matched with the users who pass the first level of authentication, for example, Face + PIN.

Note

- This feature is not used for Public PIN and Apartment+PIN.

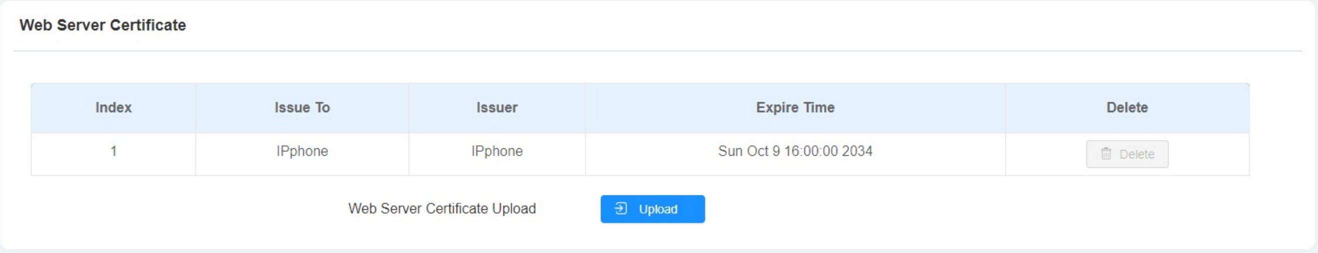
Client Certificate Setting

Certificates ensure communication integrity and privacy. To use the SSL protocol, you need to upload the right certificates for verification.

Web Server Certificate

It is a certificate sent to the client for authentication when the client requests an SSL connection with the Akuvox door phone. Please upload the certificates in accepted formats.

To upload a Web Server certificate on the device web **System > Certificate > Web Server Certificate**.



Web Server Certificate

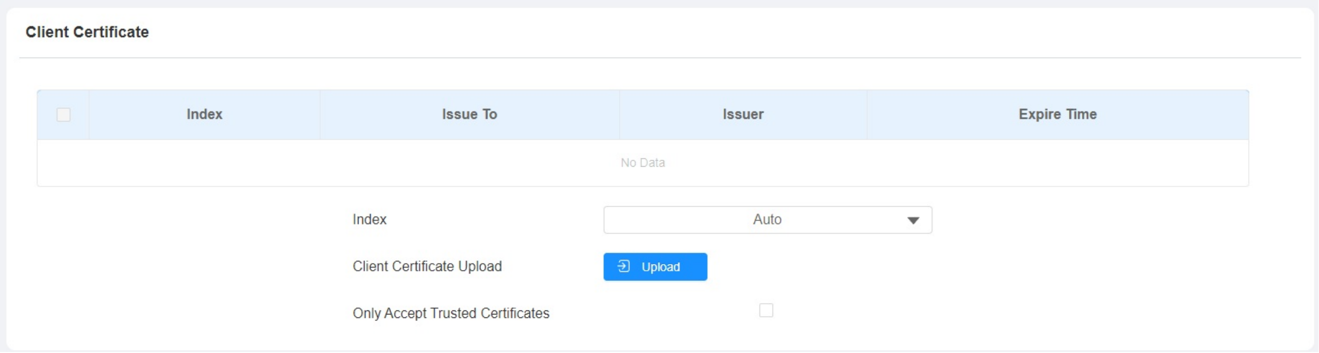
Index	Issue To	Issuer	Expire Time	Delete
1	IPphone	IPphone	Sun Oct 9 16:00:00 2034	Delete

Web Server Certificate Upload

Client Certificate

This certificate verifies the server to the Akuvox door phone when they want to connect using SSL. The door phone verifies the server's certificate against its client certificate list.

To upload and configure client certificates on the same page.



Client Certificate

☐	Index	Issue To	Issuer	Expire Time
No Data				

Index: Auto

Client Certificate Upload: Upload

Only Accept Trusted Certificates: ☐

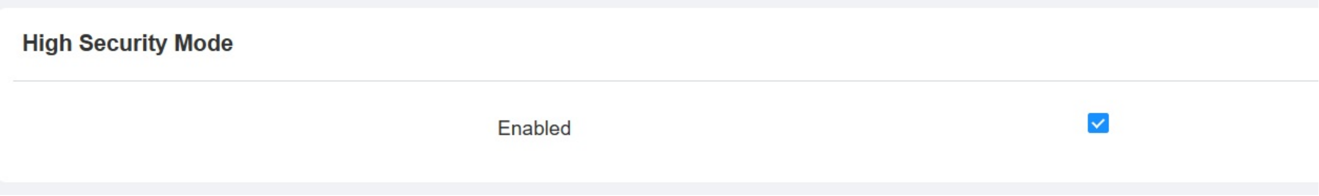
Parameter Set-up:

- **Index**: select the desired value from the drop-down list of Index. If you select **Auto** value, the uploaded certificate will be displayed in numeric order. If you select the value from **1** to **10**, the uploaded certificate will be displayed according to the value that the user selected.
- **Client Certificate Upload**: locate and upload the desired certificate (*.pem only).
- **Only Accept Trusted Certificates**: if you select **Enabled**, as long as the authentication success, the phone will verify the server certificate based on the client certificate list. If you select **Disabled**, the phone will not verify the server certificate no matter whether the certificate is valid or not.

High Security Mode

High security mode is designed to enhance the security. It employs encryption across various facets, including the communication process, door opening commands, password storage methods, and more.

To configure it on the web **System > Security > High Security Mode** interface.



High Security Mode

Enabled ☑

Important Notes

1. The High Security mode is off by default when you upgrade the device from a version without the mode to one with it. But if you reset the device to its factory settings, the mode is on by default.

2. This mode makes the old version tools incompatible. You need to upgrade them to the following versions or higher to use them.

·PC Manager: 1.2.0.0

·IP Scanner: 2.2.0.0

·Upgrade Tool: 4.1.0.0

·SDMC: 6.0.0.34

3. The supported HTTP format for relay triggering varies depending on whether high secure mode is enabled or disabled.

If the mode is on, the device only accepts the new HTTP formats below for door opening.

- l http://username:password@deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1
- l http://deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1

If the mode is off, the device can use both the new formats above and the old format below:

- l http://deviceIP/fcgi/do?action=OpenDoor&UserName=username&Password=password&DoorNum=1

4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

Monitor and Image

MJPEG and RTSP are the primary monitoring stream types discussed in this chapter.

MJPEG, or Motion JPEG, is a video compression format that uses JPEG images for each video frame. Akuvox devices display live streams on the web interface and capture monitoring screenshots in MJPEG format. Settings related to MJPEG determine video quality and the on/off status of the live stream function.

RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

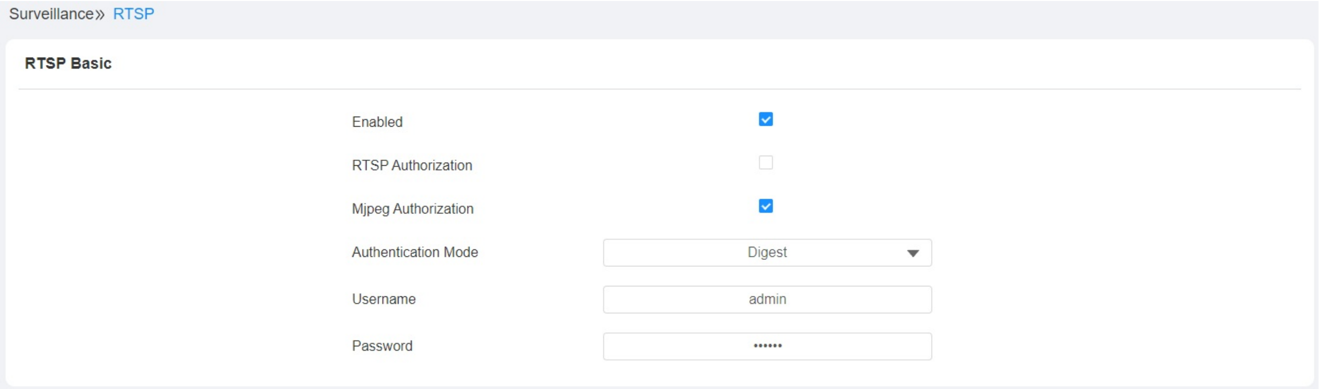
ONVIF is an Open Network Video Interface Forum. It enables the device to scan and discover cameras or intercom devices with activated ONVIF functions. Live streams obtained through ONVIF are essentially in RTSP format.

RTSP Stream Monitoring

You can use RTSP to watch a live video stream from other intercom devices on the device.

RTSP Basic Setting

To configure it on the web **Surveillance > RTSP > RTSP Basic**.



Surveillance» RTSP

RTSP Basic

Enabled	☑
RTSP Authorization	□
Mjpeg Authorization	☑
Authentication Mode	Digest
Username	admin
Password	••••••

Parameter Set-up:

- **RTSP Authorization**: enable the RTSP authorization. If you enable the RTSP Authorization, you are required to enter RTSP Authentication Type, RTSP Username, and

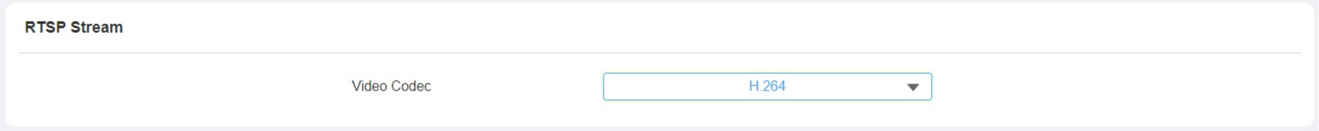
RTSP Password on the intercom device such as an indoor monitor for authorization.

- **Authentication Mode**: select the RTSP authentication type between **Basic** and **Digest**. **Basic** is the default authentication type.

RTSP Stream Setting

The RTSP stream can use either H.264 or Mjpeg as the video codec. If you choose H.264, you can also adjust the video resolution, bitrate, and other settings.

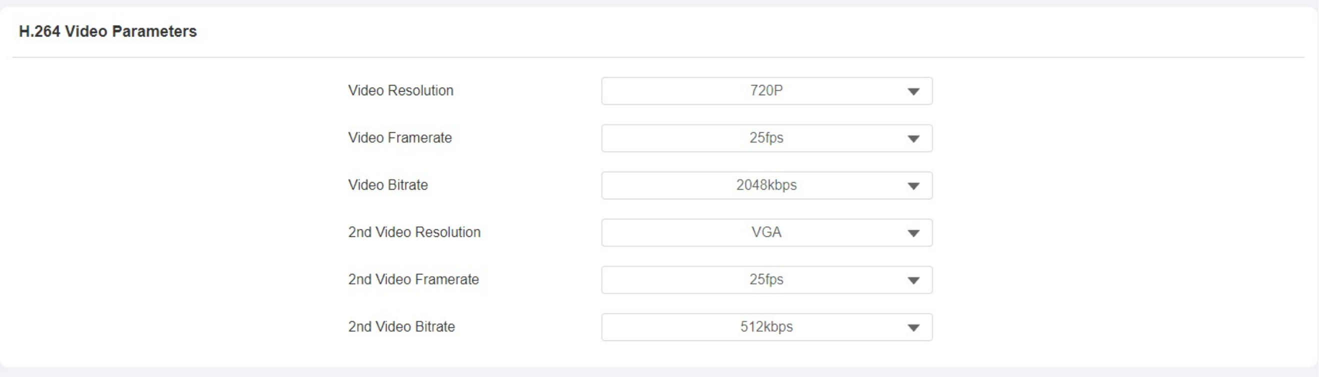
Navigate to **Surveillance > RTSP > RTSP Stream** interface.



RTSP Stream

Video Codec: H.264

To configure the parameters for H.264 codec on the web **Surveillance > RTSP > H.264 Video Parameters** interface.



H.264 Video Parameters

Video Resolution: 720P
Video Framerate: 25fps
Video Bitrate: 2048kbps
2nd Video Resolution: VGA
2nd Video Framerate: 25fps
2nd Video Bitrate: 512kbps

Parameter Set-up:

- **Video Resolution**: select video resolutions among seven options: **QCIF, QVGA, CIF, VGA, 4CIF, 720P**, and **1080P**. The default video resolution is that the video from the door phone might not be able to be shown on the indoor monitor if the resolution is set higher than **720P**.
- **Video Framerate**: **25fps** is the video frame rate by default.
- **Video Bitrate**: select video bitrate among six options: **128 kbps, 256 kbps, 512 kbps, 1024 kbps, 2048 kbps**, and **4096 kbps** according to your network environment. The default video bitrate is **2048 kbps**.
- **2nd Video Resolution**: select the video resolution for the second video stream channel. While the default video solution is **VGA**.
- **2nd Video Framerate**: select the video framerate for the second video stream channel.

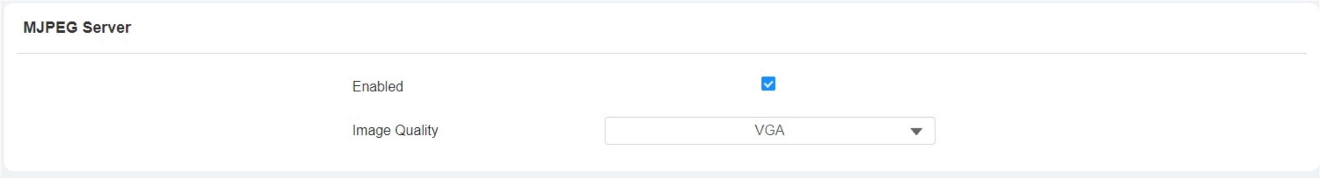
25fps is the default video frame rate for the second video stream channel.

- **2nd Video Bitrate**: select video bitrate among the six options for the second video stream channel. While the second video stream channel is **512 kbps** by default.

MJPEG Image Capturing

You can take a monitoring image in Mjpeg format with the device. To do this, you need to turn on the Mjpeg function and choose the image quality.

Navigate to **Surveillance > MJPEG** interface.



MJPEG Server

Enabled ☑

Image Quality VGA

Parameter Set-up:

- **Image Quality**: select the quality for the image capturing among seven options: QCIF, QVGA, CIF, VGA, 4CIF, 720P, 1080P

After the MJPEG service is enabled, you can capture the image from the door phone using the following three types of URL format:

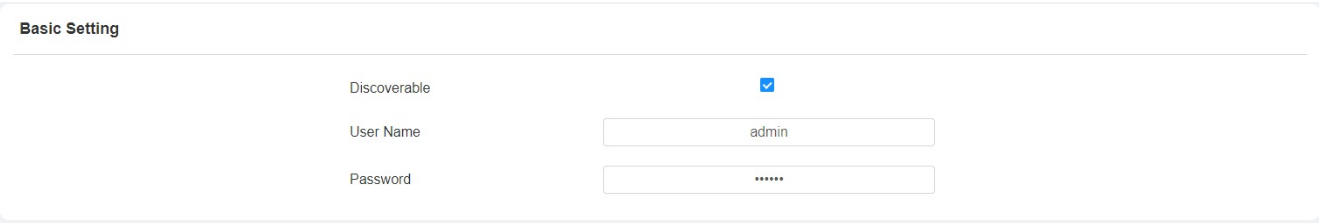
- http:// device ip:8080/picture.cgi
- http://deviceip:8080/picture.jpg
- http://deviceip:8080/jpeg.cgi

For example, if you want to capture the JPG format image of a door phone with the IP address: 192.168.1.104, you can enter “http://192.168.1.104:8080/picture.jpg” on the web browser.

ONVIF

You can access the real-time video from the device's camera using the Akuvox indoor monitor or other third-party devices like Network Video Recorder(**NVR**). Enabling and setting up the ONVIF function on the device will allow its video to be visible on other devices.

To configure on the web **Surveillance > ONVIF > Basic Setting** interface.



Basic Setting

Discoverable ☑

User Name: admin

Password: ••••••

Parameter Set-up:

- **Discoverable**: tick the check box to enable the Discoverable ONVIF mode. If you select **Discoverable** then the video from the door phone camera can be searched by other devices.
- **User Name**: enter the user name. The user name is **admin** by default.
- **Password**: enter the password. The password is **admin **by default.

After the setting is complete, you can enter the ONVIF URL on the third-party device to view the video stream.

For example: **http://IP address:80/onvif/device_service**

Note

- Fill in the specific IP address of the door phone in the URL.

Live Stream

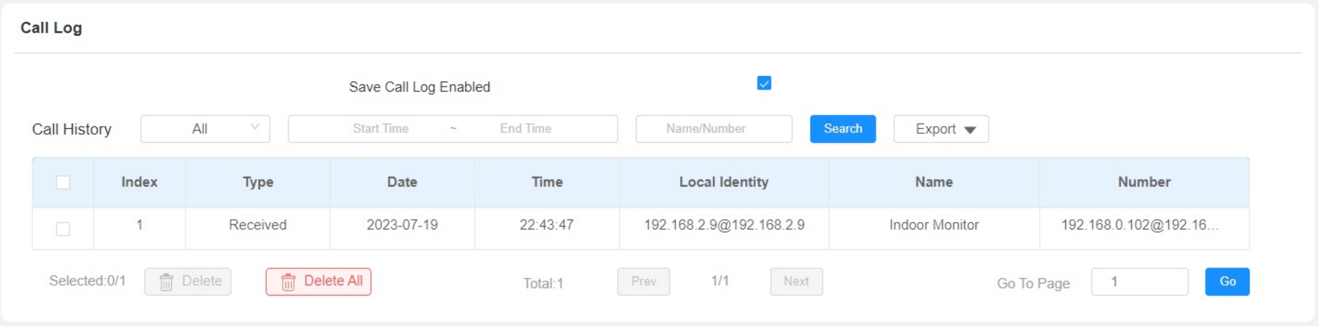
There are two ways to check the real-time video from the device. One is to go to the device web interface and view the video there. The other is to enter the correct URL on the web browser and access the video directly.

Logs

Call Logs

If you want to check on the calls inclusive of the dial-out calls, received calls, and missed calls in a certain period of time, you can check and search the call log on the device web interface and export the call log from the device if needed.

To check the call log on the web **Status > Call Log**.



Call Log

Save Call Log Enabled ☑

Call History All Start Time ~ End Time Name/Number Search Export

□	Index	Type	Date	Time	Local Identity	Name	Number
□	1	Received	2023-07-19	22:43:47	192.168.2.9@192.168.2.9	Indoor Monitor	192.168.0.102@192.16...

Selected:0/1 Delete Delete All Total:1 Prev 1/1 Next Go To Page 1 Go

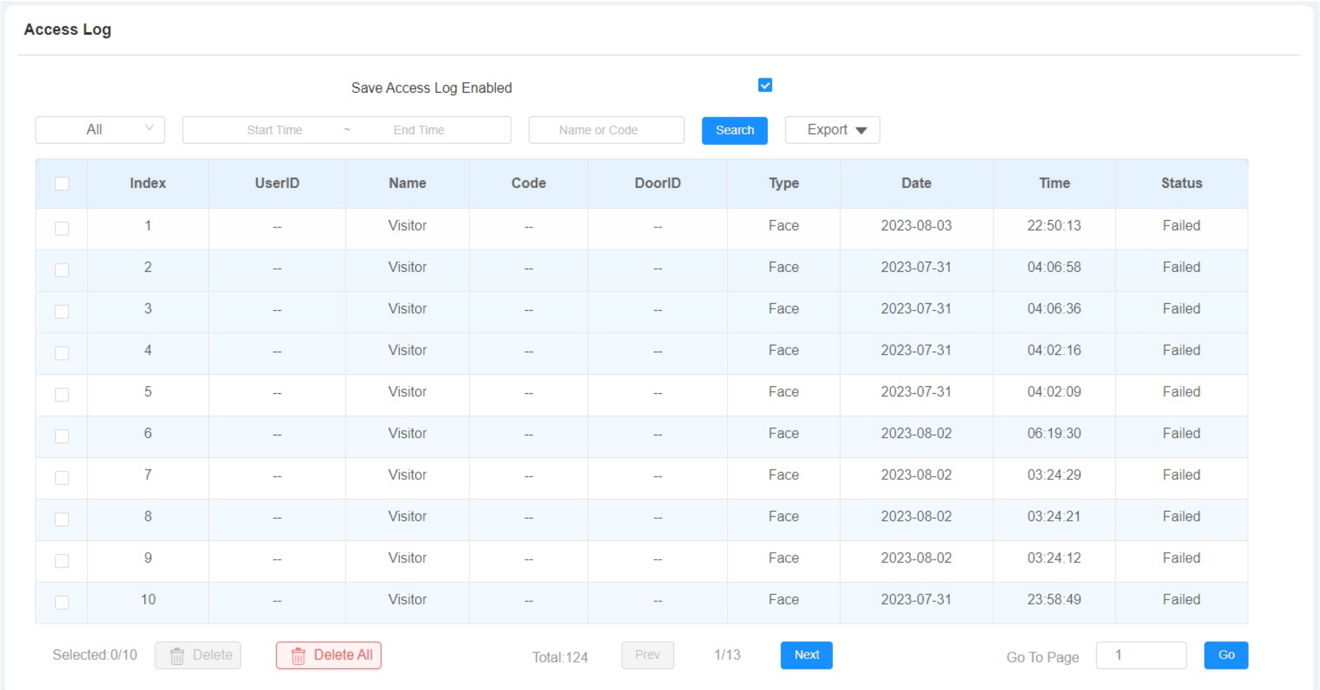
Parameter Set-up:

- **Call History**: select call history among four options: **All, Dialed, Received**, and **Missed** for the specific type of call log to be displayed.
- **Start Time- End Time**: select the specific time span of the call logs you want to search, check, or export.
- **Name/Number**: select the **Name** and **Number** options to search call log by the name or by the SIP or IP number.

Door Logs

If you want to search and check on the various types of door access history, you can search and check the door logs on the device's web.

Go to **Status > Access Log** interface.



Access Log

Save Access Log Enabled ☑

All ˅ | Start Time ~ End Time | Name or Code | Search | Export ▾

□	Index	UserID	Name	Code	DoorID	Type	Date	Time	Status
□	1	--	Visitor	--	--	Face	2023-08-03	22:50:13	Failed
□	2	--	Visitor	--	--	Face	2023-07-31	04:06:58	Failed
□	3	--	Visitor	--	--	Face	2023-07-31	04:06:36	Failed
□	4	--	Visitor	--	--	Face	2023-07-31	04:02:16	Failed
□	5	--	Visitor	--	--	Face	2023-07-31	04:02:09	Failed
□	6	--	Visitor	--	--	Face	2023-08-02	06:19:30	Failed
□	7	--	Visitor	--	--	Face	2023-08-02	03:24:29	Failed
□	8	--	Visitor	--	--	Face	2023-08-02	03:24:21	Failed
□	9	--	Visitor	--	--	Face	2023-08-02	03:24:12	Failed
□	10	--	Visitor	--	--	Face	2023-07-31	23:58:49	Failed

Selected:0/10 | Delete | Delete All | Total:124 | Prev | 1/13 | Next | Go To Page 1 | Go

Parameter Set-up:

- **Status**: Select between **Success** and **Failed** options to search for successful door accesses or Failed door accesses.
- **Start Time~ End Time**: select the specific time span of the door logs you want to search, check, or export.
- **Name/Code**: select the **Name** and **Code** options to search the door log by the name or by the PIN code.

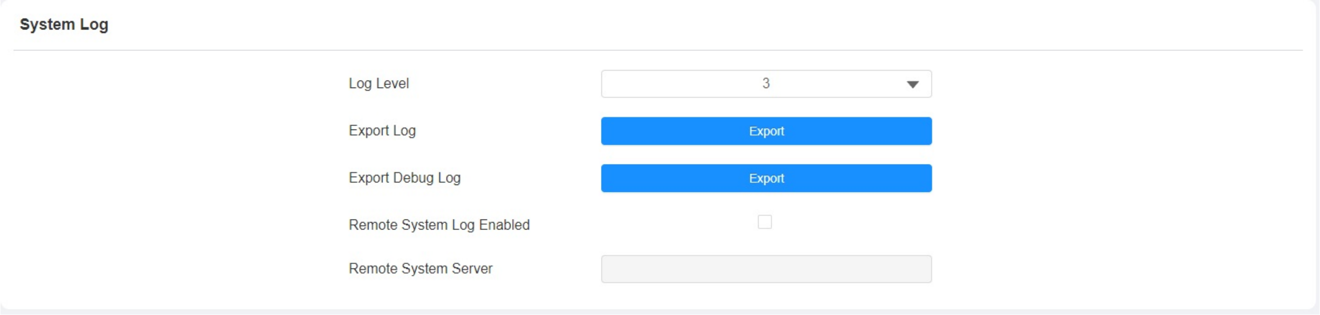
Debug

System Log for Debugging

System logs can be used for debugging purposes.

You can export the system out to a local PC or to a remote server for debugging.

To set up the function on the web **System** > **Maintenance** > **System Log** interface.



System Log

Log Level: 3

Export Log: Export

Export Debug Log: Export

Remote System Log Enabled: □

Remote System Server:

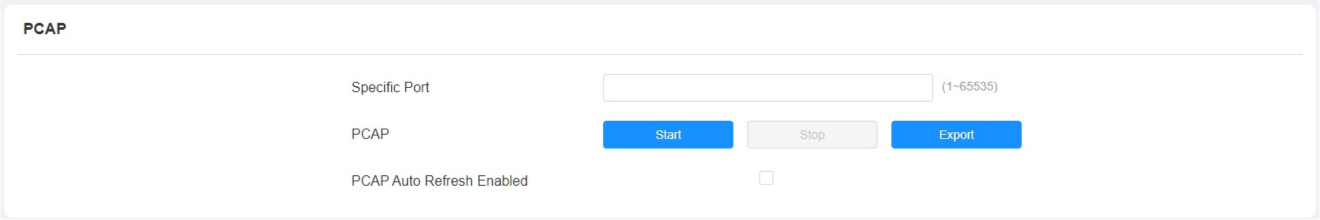
Parameter Set-up:

- **Log Level**: select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Remote System Server**: enter the remote server address to receive the device. And the remote server address will be provided by Akuvox technical support.

PCAP for Debugging

PCAP is used to capture the data package going in and out of the devices for debugging and troubleshooting purposes.

You can set up the PCAP on the device web **System** > **Maintenance** > **PCAP** interface properly before using it.



PCAP

Specific Port: (1~65535)

PCAP: Start Stop Export

PCAP Auto Refresh Enabled: □

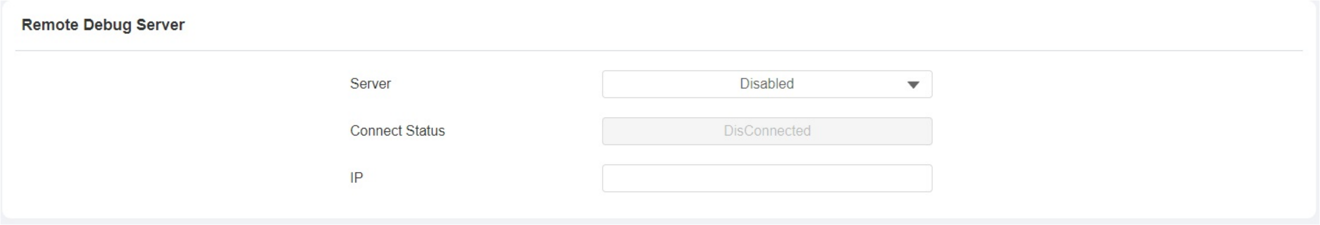
Parameter Set-up:

- **Specific Port**: select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP**: click the **Start** tab and **Stop** tab to capture a certain range of data packets before clicking the **Export** tab to export the data packets to your Local PC.
- **PCAP Auto Refresh**: if you enable the feature, then the PCAP will continue to capture data packets even after the data packets reached 1M maximum in capacity. If you disenable it, the PCAP will stop data packet capturing when the data packet captured reached the maximum capturing capacity of 1MB.

Remote Debug Server

When the device is having a problem, you can use the remote debug server to access the device log remotely for debugging purposes.

On the web, navigate to **System > Maintenance > Remote Debug Server** interface.



Remote Debug Server

Server	Disabled
Connect Status	DisConnected
IP	

Parameter Set-up:

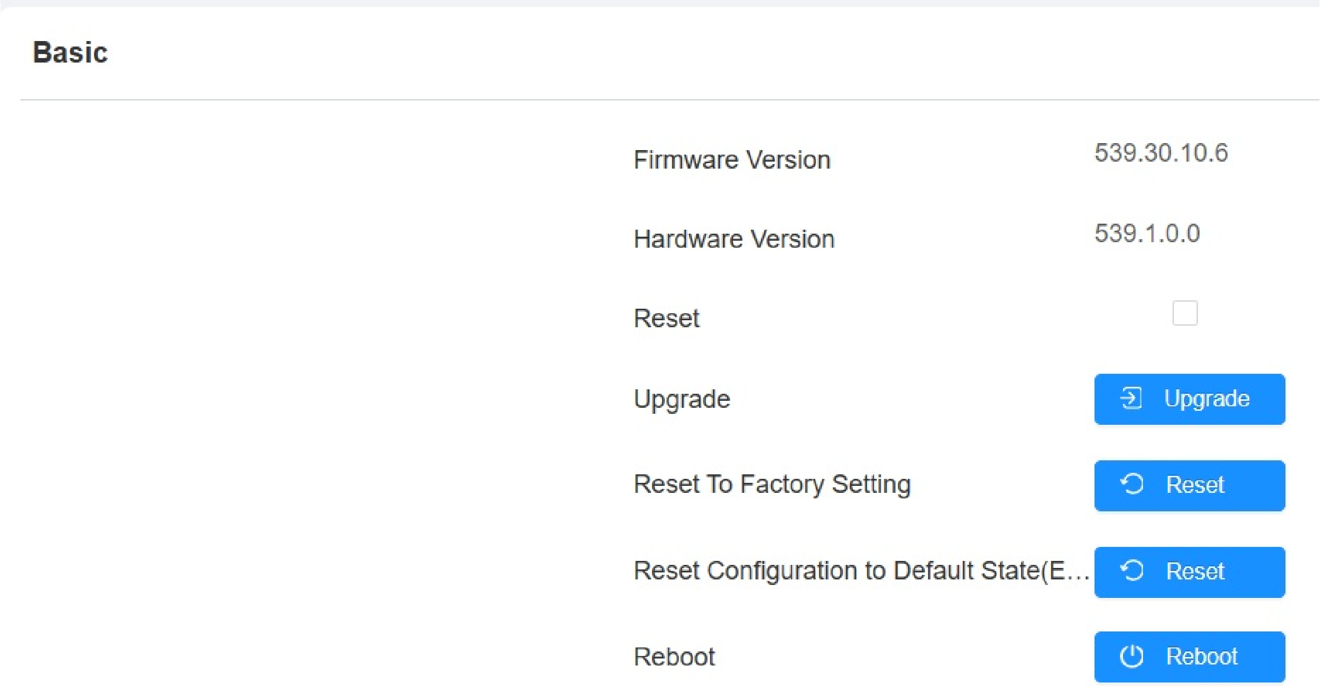
- **IP**: enter the remote debug server IP address. Please ask Akuvox technical team for the server IP address.

> **Note**
>
> - You are required to send the door phone’s MAC address to the Akuvox technical team.

Firmware Upgrade

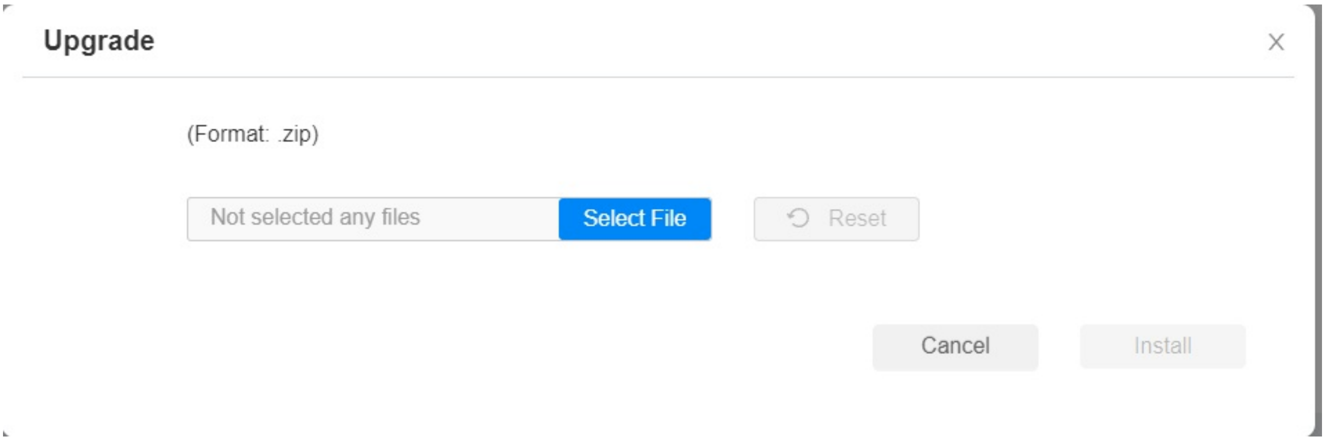
Akuvox devices can be upgraded on the device web interface.

You can go to **System> Upgrade** interface.



Basic

Firmware Version	539.30.10.6
Hardware Version	539.1.0.0
Reset	□
Upgrade	Upgrade
Reset To Factory Setting	Reset
Reset Configuration to Default State(E…	Reset
Reboot	Reboot



Upgrade

(Format: .zip)

Not selected any files

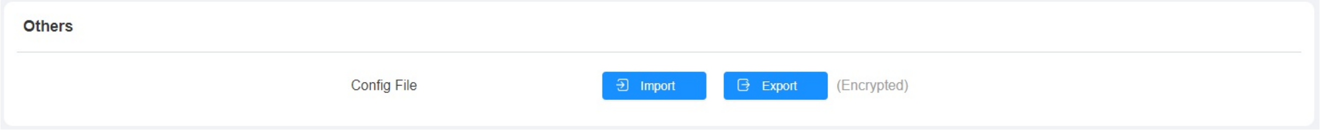
Note

- Firmware files should be in **.zip** format for the upgrade.

Backup

You can import or export encrypted configuration files to your Local PC.

Go to **System** > **Maintenance** > **Others** interface.



Auto-provisioning

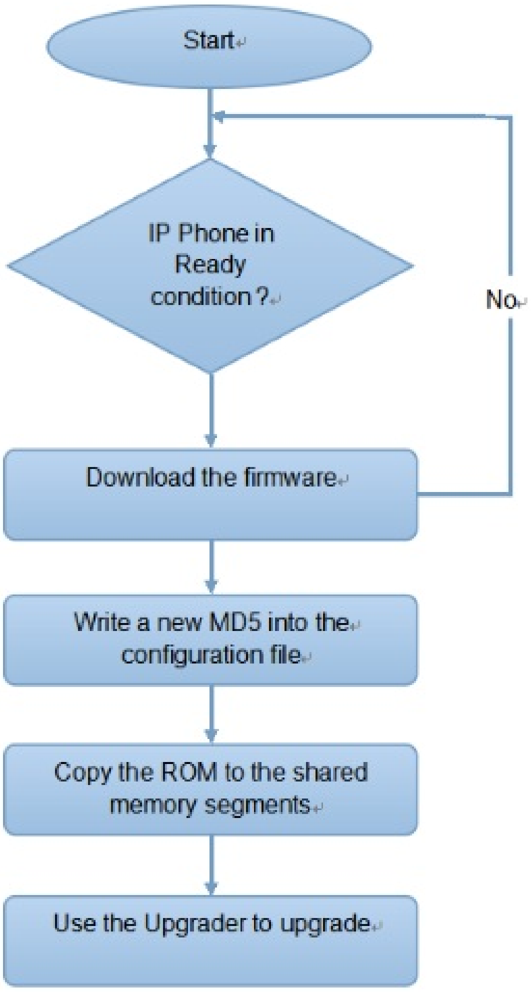
Auto-provisioning via Configuration File

You can configure and upgrade the door phone on the web interface via one-time auto- provisioning and scheduled auto-provisioning via configuration files, thus saving you from setting up configurations needed one by one manually on the door phone.

Provisioning Principle

Auto-provisioning is a feature used to configure or upgrade devices in batch via third-party servers. **DHCP, PNP, TFTP, FTP, and HTTPS** are the protocols used by the Akuvox devices to access the URL of the address of the third-party server which stores configuration files and firmware, which will then be used to update the firmware and the corresponding parameters on the device.

Please see the flow chart below:


Start
IP Phone in Ready condition ?
No
Download the firmware
Write a new MD5 into the configuration file
Copy the ROM to the shared memory segments
Use the Upgrader to upgrade

Configuration Files for Auto-provisioning

Configuration files have two formats for auto-provisioning. One is the general configuration files used for the general provisioning and the other one is the MAC-based configuration provisioning.

The difference between the two types of configuration files is shown below:

- **General configuration provisioning**: a general file is stored in a server from which all the related devices will be able to download the same configuration file to update parameters on the devices, such as cfg.
- **MAC-based configuration provisioning**: MAC-based configuration files are used for auto-provisioning on a specific device, as distinguished by its unique MAC number. The configuration files named with the device MAC number will be matched automatically with the device MAC number before being downloaded for provisioning on the specific device.

Note

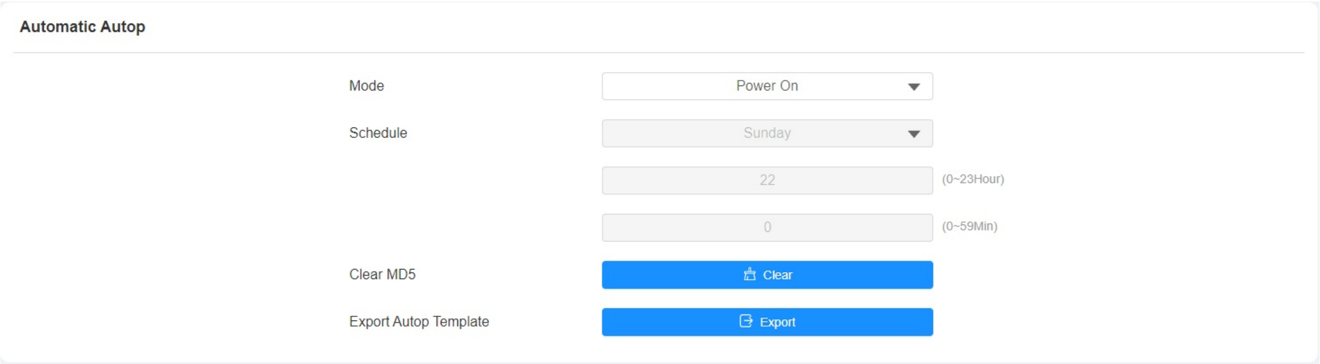
- The configuration file should be in CFG format.
- The general configuration file for the in-batch provisioning varies by model.
- The MAC-based configuration file for the specific device provisioning is named by its MAC address.
- If a server has these two types of configuration files, devices will first access the general configuration files before accessing the MAC-based configuration files.

You may click here to see the detailed format and steps.

Auto Provision Schedule

Akuvox provides you with different AutoP methods that enable the door phone to perform provisioning for itself at a specific time according to your schedule.

To configure it, go to **System** > **Auto Provisioning** > **Automatic Autop** interface.



Automatic Autop

Mode: Power On

Schedule: Sunday

22 (0~23Hour)

0 (0~59Min)

Clear MD5

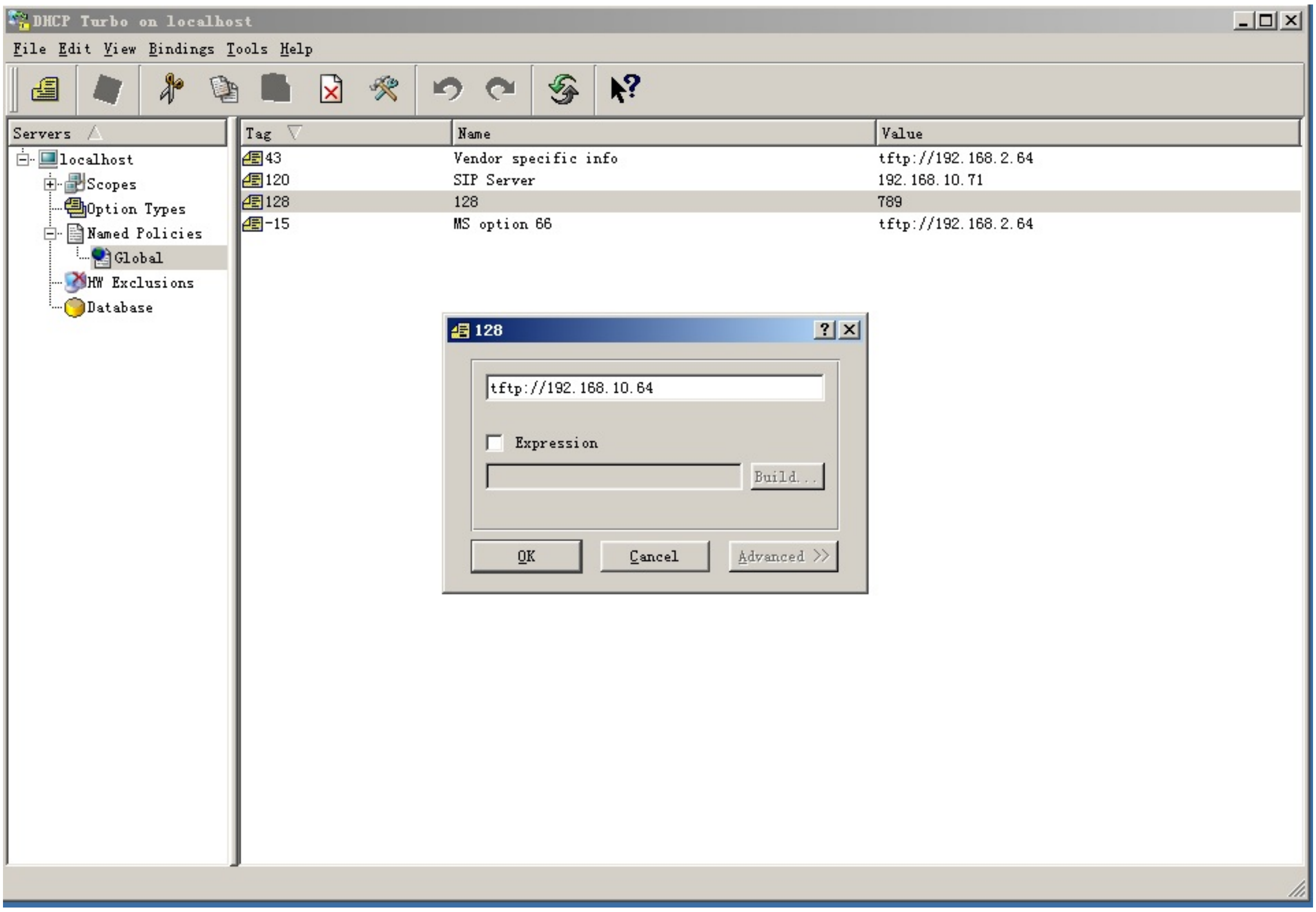
Export Autop Template

Parameter Set-up:

- **Mode**: Select **Power on, Repeatedly, Power On + Repeatedly**, and **Hourly Repeat** as your AutoP schedule.
    - Select **Power on** if you want the device to perform AutoP every time it boots up.
    - Select **Repeatedly**, if you want the device to perform AutoP according to the schedule you set up.
    - Select **Power On + Repeatedly** if you want to combine **Power On** mode and **Repeatedly** mode, it would enable the device to perform AutoP every time it boots up or according to the schedule you set up.
    - Select **Hourly Repeat** if you want the device to perform AutoP every hour.

DHCP Provisioning Configuration

Auto-provisioning URL can also be obtained using the DHCP option which allows the device to send a request to a DHCP server for a specific DHCP option code. If you want to use **Custom Option** as defined by users with option codes ranging from 128-255), you are required to configure DHCP Custom Option on the web interface.



Tag	Name	Value
43	Vendor specific info	tftp://192.168.2.64
120	SIP Server	192.168.10.71
128	128	789
-15	MS option 66	tftp://192.168.2.64

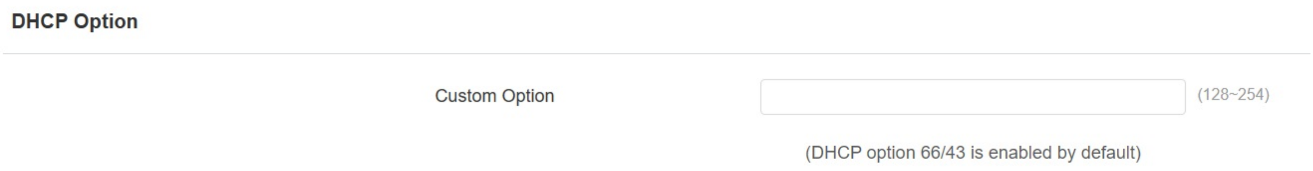
128

tftp://192.168.10.64

□ Expression

> **Note**
>
> - The Custom Option type must be a string. The value is the URL of TFTP server.

Navigate to **System > Auto Provisioning** interface.



DHCP Option

Custom Option (128~254)

(DHCP option 66/43 is enabled by default)

Parameter Set-up:

- **Custom Option**: enter the DHCP code that matched the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 66**: If none of the above is set, the device will automatically use DHCP Option 66 for getting the upgrade server URL. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 66 with the updated server URL in it.
- **DHCP Option 43**: If the device does not get an URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 43 with the updated server URL in it.

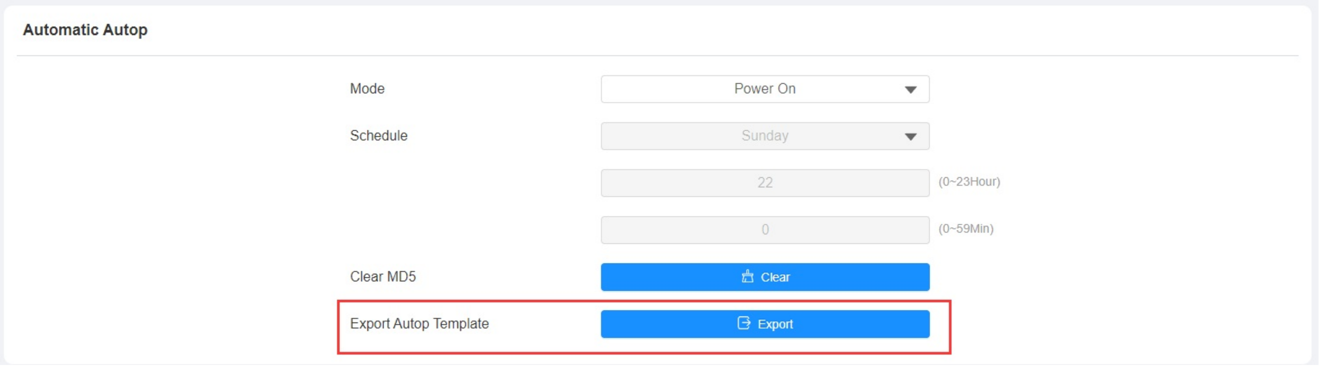
Note

- The general configuration file for the in-batch provisioning is in the format **r0000000000xx.cfg**. Taking X915 as an example r000000000915.cfg (**10 zeros** in total while the MAC-based configuration file for the specific device provisioning is with the format MAC Address of the device.cfg, for example, **0C110504AE5B.cfg**).
- You can upload the screen saver by Auto-provisioning.

Static Provisioning Configuration

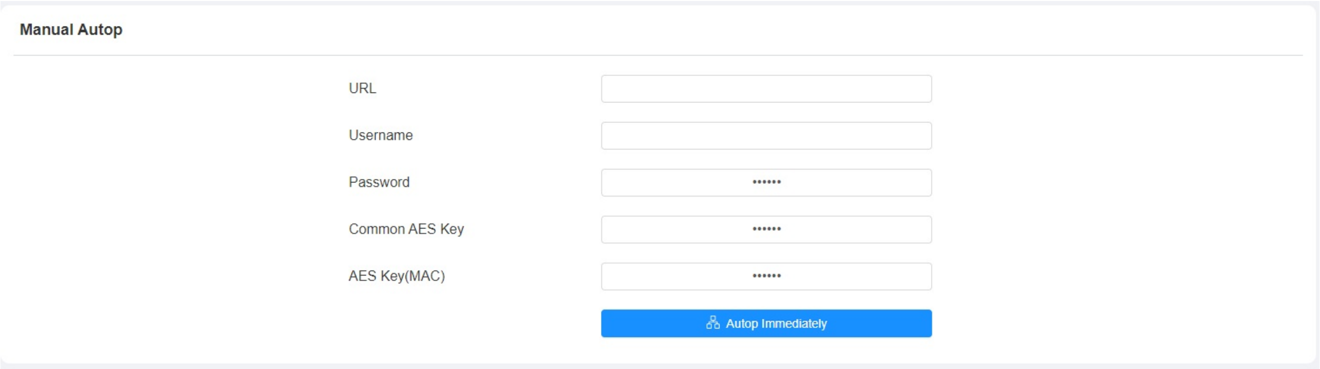
You can manually set up a specific server URL for downloading the firmware or configuration file. If an auto-provision schedule is set up, the device will perform the auto-provisioning at a specific time according to the auto provision schedule you set up. In addition, TFTP, FTP, HTTP, and HTTPS are the protocols that can be used for upgrading the device firmware and configuration.

To download the AutoP template on **System > Auto Provisioning > Automatic Autop**, and set up the Auto provisioning server on **System > Auto Provisioning > Manual Autop** interface.



Automatic Autop

Mode	Power On
Schedule	Sunday
	22 (0~23Hour)
	0 (0~59Min)
Clear MD5	Clear
Export Autop Template	Export



Manual Autop

URL	
Username	
Password	••••••
Common AES Key	••••••
AES Key(MAC)	••••••

Parameter Set-up:

- **URL**: set up TFTP, HTTP, HTTPS, FTP server addresses for the provisioning
- **User Name**: set up a user name the server needs a user name to be accessed if needed.
- **Password**: set up a password if the server needs a password to be accessed if needed.
- **Common AES Key**: set up AES code for the intercom to decipher the general Auto Provisioning configuration files.
- **AES Key (MAC)**: set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

Note

- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(allows anonymous login)
    ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/(use the default port 80)
    http://192.168.0.19:8080/(use other ports, such as 8080)
  - HTTPS: https://192.168.0.19/(use the default port 443)

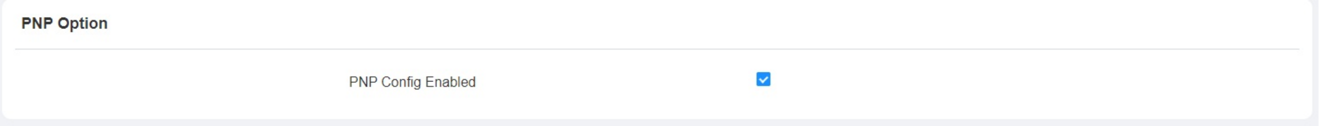
Tip

- Akuvox do not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

PNP Configuration

Plug and Play (PNP) is a combination of hardware and software support that enables a computer system to recognize and adapt to hardware configuration changes with little or no intervention by a user.

To configure on the web **System > Auto Provisioning > PNP Option** interface.



PNP Option

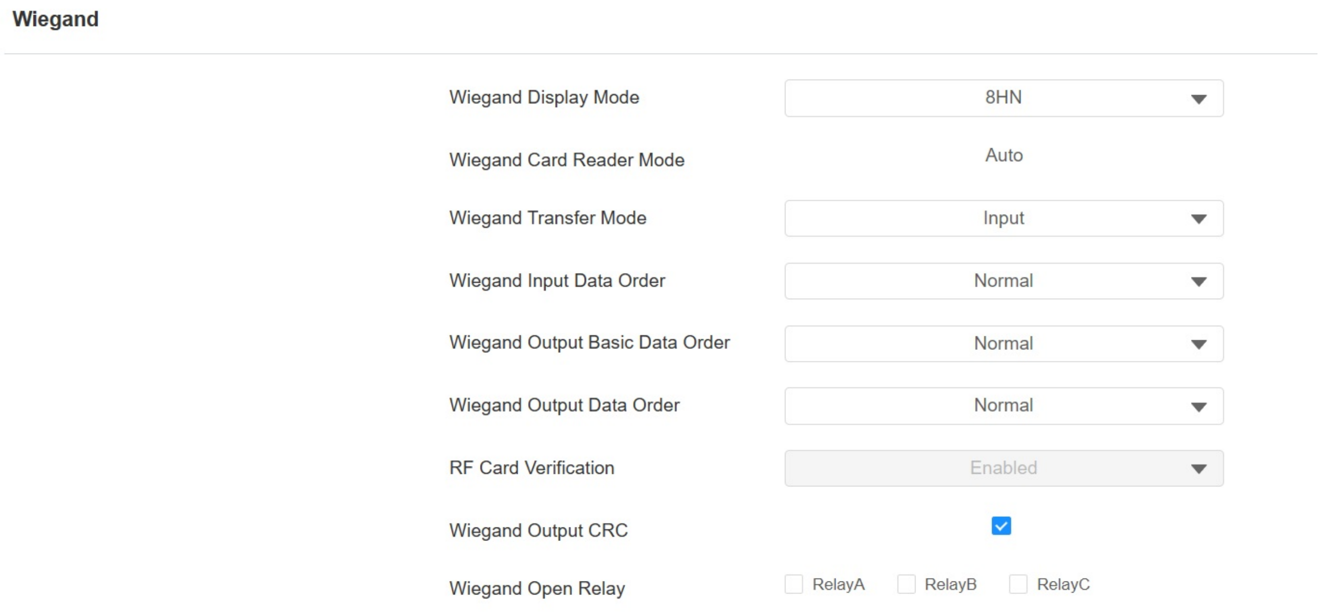
PNP Config Enabled ☑

Integration with Third Party Device

Integration via Wiegand

The Wiegand feature enables Akuvox door phone to act as a controller or a card reader.

you can configure it on the web **Device** > **Wiegand** interface.



Wiegand

Wiegand Display Mode	8HN
Wiegand Card Reader Mode	Auto
Wiegand Transfer Mode	Input
Wiegand Input Data Order	Normal
Wiegand Output Basic Data Order	Normal
Wiegand Output Data Order	Normal
RF Card Verification	Enabled
Wiegand Output CRC	☑
Wiegand Open Relay	□ RelayA □ RelayB □ RelayC

Parameter Set-up:

- **Wiegand Display Mode**: select Wiegand Card code format among **8H10D; 6H3D5D; 6H8D; 8HN; 8HR; 6H3D5D-R(W26); 8HR10D; RAW.**
- **Wiegand Card Reader Mode**: this field is dimmed and is not available for changing because the Wiegand card reader can adapt to all types of data input.
- **Wiegand Transfer Mode**: set the Transfer mode between **Input** or **Output** if the door phone is used as a receiver, then set it as Input for the door phone and vice versa.
- **Wiegand Input Data Order**: set the Wiegand input data sequence between **Normal** and **Reversed** if you select Reversed then the input card number will be reversed and vice versa.
- **Wiegand Output Basic Data Order**: select **Normal** if you want Wiegand output data to be displayed in a normal state. Select **Reversed** if you want to reverse the output data, for example from 0x110x220x330x44 to 0x440x330x220x11.
- **Wiegand Output Data Order**: set the Wiegand output data sequence between **Normal**

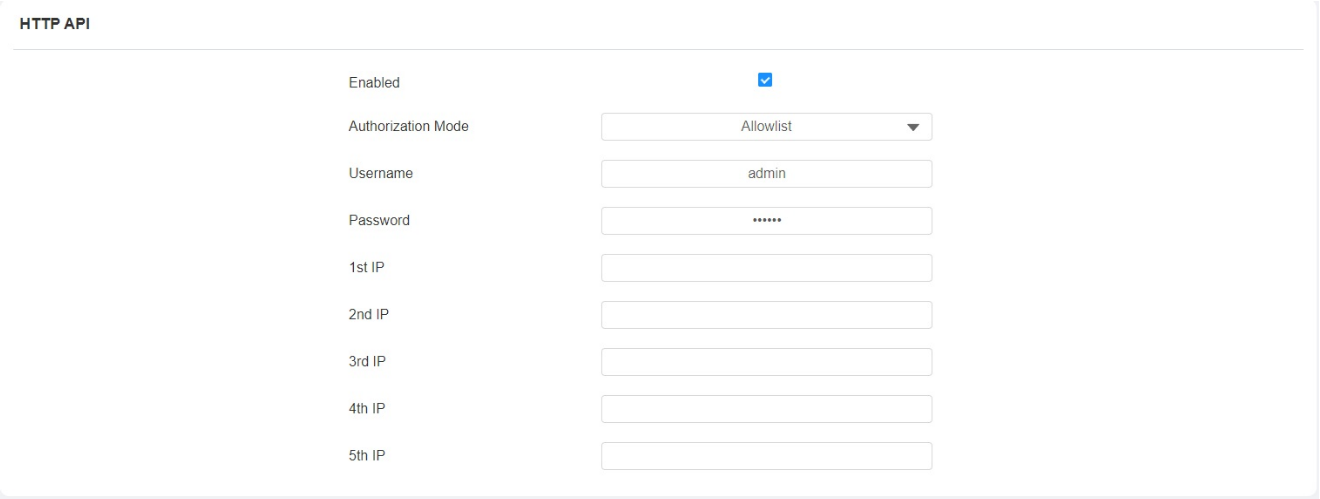
and **Reversed** if you select **Reversed** then the input card number will be reversed and vice versa.

- **Wiegand Output CRC**: This function is used for Wiegand data inspection. It is turned on by default. If it is not turned on, you might not be able to integrate the device with third-party devices.

Integration via HTTP API

HTTP API is designed to achieve a network-based integration between the third-party device and the Akuvox device.

You can configure the HTTP API function on the web **Setting> HTTP API** interface for the integration.



HTTP API

Enabled	☑
Authorization Mode	Allowlist
Username	admin
Password	••••••
1st IP	
2nd IP	
3rd IP	
4th IP	
5th IP	

Parameter set-up:

- **Enabled**: enable or disable the HPTT API function for third-party integration. For example, if the function is disabled any request to initiate the integration will be denied and be returned HTTP 403 forbidden status.
- **Authorization Mode**: select among **None, Normal, Allowlist, Basic**, **Digest**, and **Token** for authorization type, which will be explained in detail in the following chart.
- **User Name**: enter the user name when **Basic** and **Digest** authorization mode is selected. The default user name is **admin.**
- **Password**: enter the password when **Basic** and **Digest** authorization mode is selected. The default password is admin.
- **1st IP-5th IP**: enter the IP address of the third-party devices when the **Allowlist** authorization is selected for the integration.

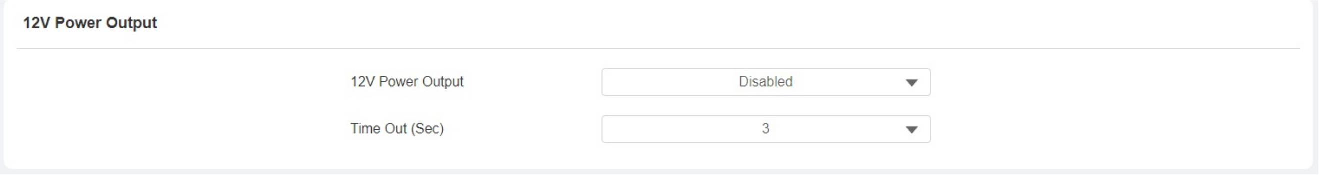
Please refer to the following description for the Authentication mode:

NO.	Authorization Mode	Description
1	None	No authentication is required for HTTP API as it is only used for demo testing.
2	Normal	This mode is used by Akuvox developer only
3	Allowlist	If this mode is selected, you are only required to fill in the IP address of the third party device for the authentication. The allowlist is suitable for operation in the LAN.
4	Basic	If this mode is selected, you are required to fill in the username and the password for the authentication. In Authorization field of HTTP request header, use Base64 encode method to encode of username and password.
5	Digest	Password encryption method, only supports MD5. MD5(Message-Digest Algorithm) In Authorization field of HTTP request header: WWW-Authenticate:Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".
6	Token	This mode is used by Akuvox developer only.

Power Output Control

The device can serve as a power supply for the external relays.

You can go to **Access Control > Relay > 12V Power Output** interface.



12V Power Output

12V Power Output: Disabled

Time Out (Sec): 3

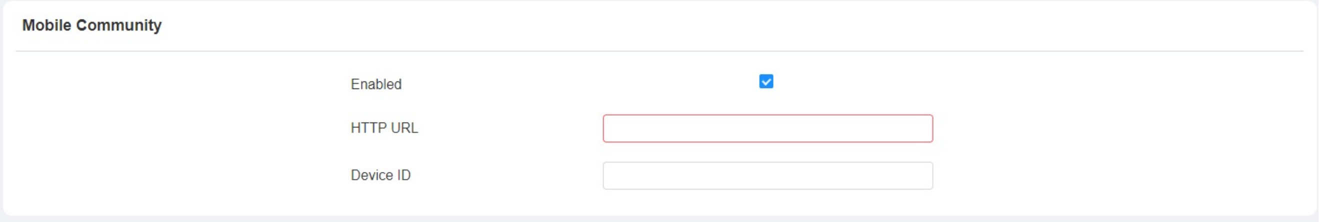
Parameter Set-up:

- **12V Power Output**: select **Disabled** to disable the power output function; select **Always** to enable the access controller to provide continuous power to the third-party device. Select **Triggered By Open Relay** if you want the door phone to provide power to the third-party device via 12 output and GND interface during the timeout when the status of relays is shifted from low to high. Select **Security Relay A** to power security relay.
- **Time Out (Sec)**: select the power supply time duration after the relay is triggered. Three options: 3, 5, 10. It is 3 seconds by default. The power output is 12V, and the maximum output amperage is 0.8A.

Mobile Community

You can connect the door phone to the third-party QR code server for QR code verification. When you access the door using a QR code, the QR code will be sent to the QR code server for verification before granting you an access permission. This feature is applied to the devices not deployed in the SmartPlus platform for the QR code door access.

You can navigate to **Access Control > Relay > Mobile Community** interface.



Mobile Community

Enabled ☑

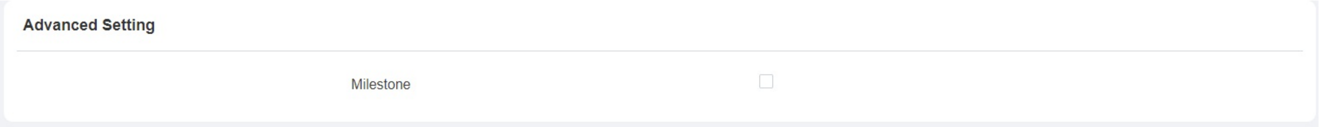
HTTP URL

Device ID

Integration with Milestone

If you want the door phone to be monitored by Milestone or any third-party devices that have been integrated with Milestone, you need to enable the feature.

To do so, go to **Surveillance > ONVIF > Advanced Setting** interface.



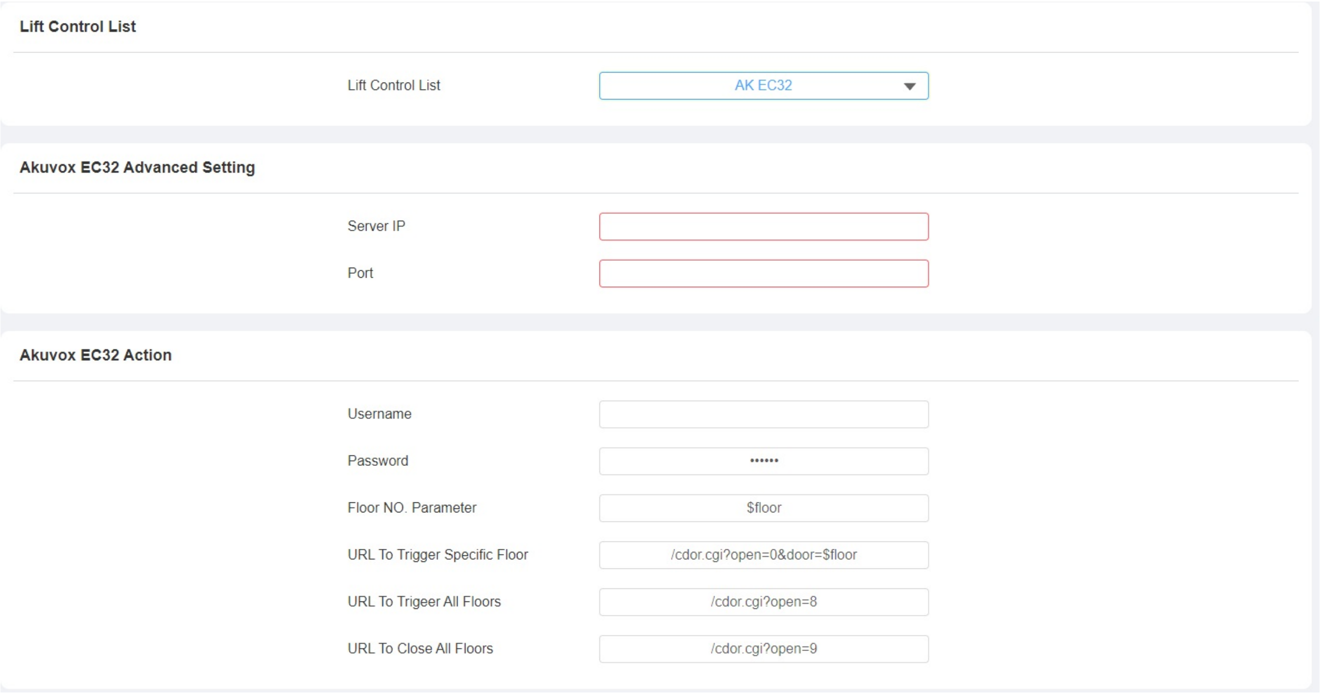
Advanced Setting

Milestone □

Lift Control

The door phones can be connected to the Akuvox lift controller for the lift control. Users can summon the lift to go down to the ground floor when they are granted access through various types of access methods on the door phone.

To set up the lift control, navigate to **Device > Lift Control** interface.



Lift Control List

Lift Control List	AK EC32

Akuvox EC32 Advanced Setting

Server IP	
Port	

Akuvox EC32 Action

Username	
Password	••••••
Floor NO. Parameter	$floor
URL To Trigger Specific Floor	/cdor.cgi?open=0&door=$floor
URL To Trigeer All Floors	/cdor.cgi?open=8
URL To Close All Floors	/cdor.cgi?open=9

Parameter Set-up:

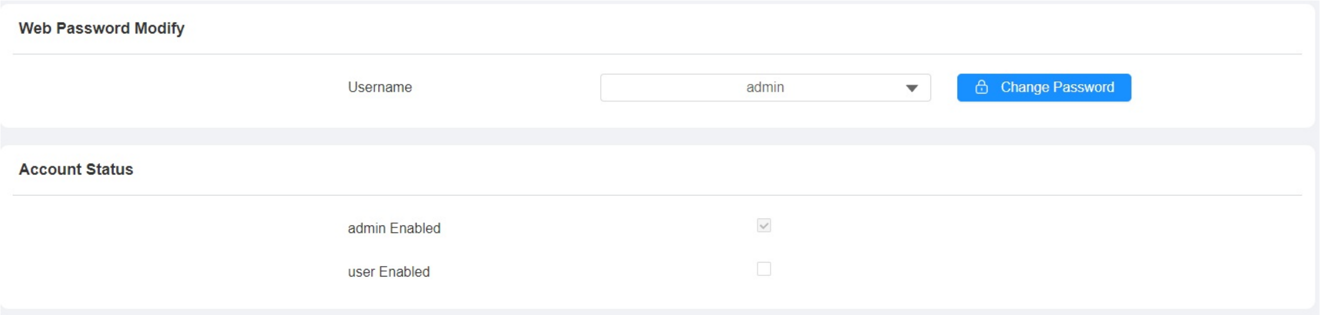
- **Lift Control List**: select **None** to disable the function, and select the Akuvox E32 to integrate the door phone with the Akuvox EC32 controller.
- **Server IP**: enter the IP address of the Akuvox EC32 controller server.
- **Server Port**: enter the Sever port of the Akuvox EC32 controller server.
- **Floor NO. Parameter**: enter the Floor number parameter provided by Akuvox. The default parameter string is "**$floor**". You can define your own parameter string if needed.
- **URL To Trigger Specific Floor**: enter the Akuvox life control URL for triggering a specific floor. The URL is **"/cdor.cgi?open=0&door=$ floor"**, but the string **"$floor"** at the end must be identical to the parameter string you defined.
- **URL To Trigger All Floors**: enter the Akuvox URL for triggering all floors.
- **URL To Close All Floors**: enter the Akuvox URL used for closing all floors, meaning all the buttons that are triggered for the corresponding floors will become invalid.

Password Modification

Modify Device Web Interface Password

To change the default web password on web **System > Security > Web Password Modify** interface.

Select **admin** for the administrator account and **User** for the User Account. Click the **Change Password** tab to change the password.



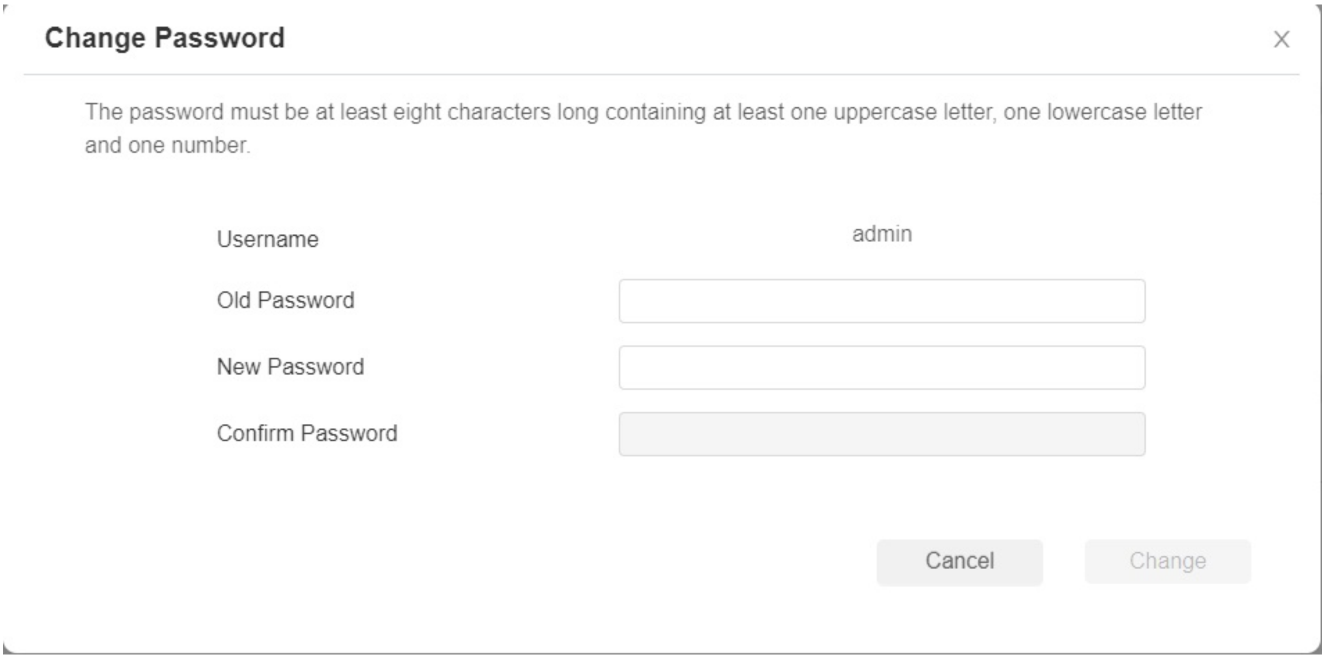
Web Password Modify

Username: admin ▾ | Change Password

Account Status

admin Enabled ☑

user Enabled □



Change Password ×

The password must be at least eight characters long containing at least one uppercase letter, one lowercase letter and one number.

Username: admin

Old Password:

New Password:

Confirm Password:

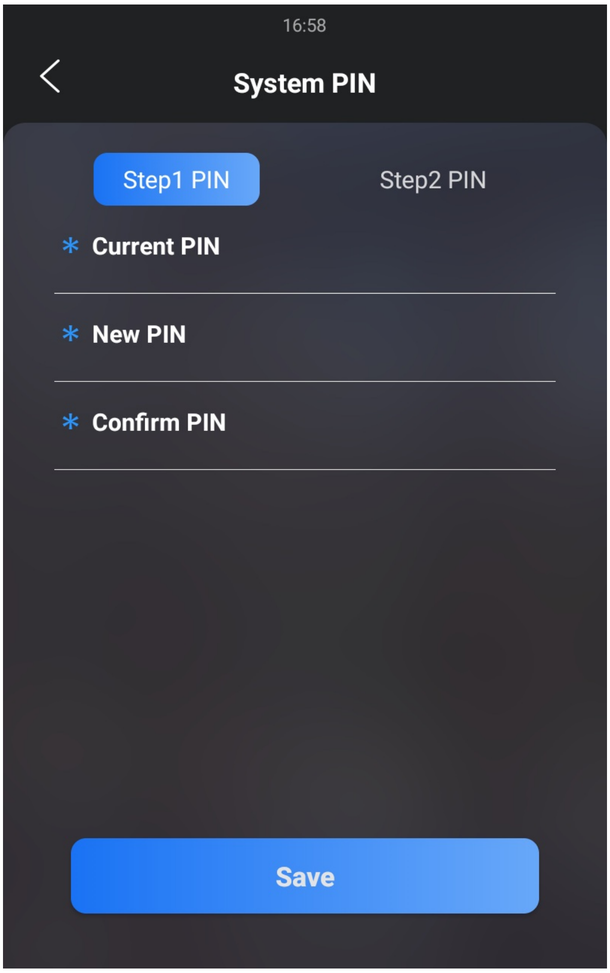
Parameter Set-up:

- **Username**: modify the admin or user password if needed.
- **User**: enable the user account if needed.

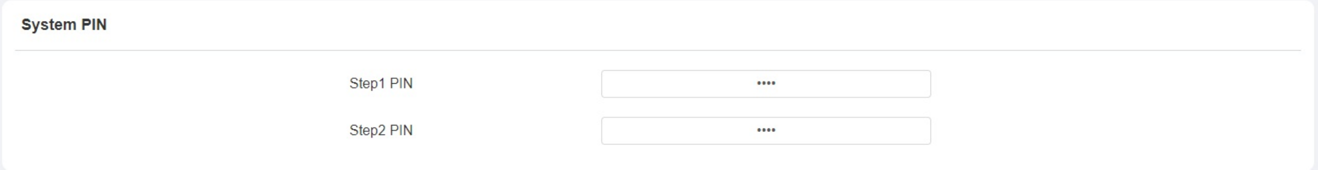
Modify System Password

The system PIN code is used to access the device system. You can modify the system PIN code on the device and web interface.

To set the system PIN code on the device, go to **Security > System PIN**, then select **Step1 PIN**.



To set up a system PIN on the web interface, navigate to **System > Security > System PIN**.



System PIN

Step1 PIN	••••
Step2 PIN	••••

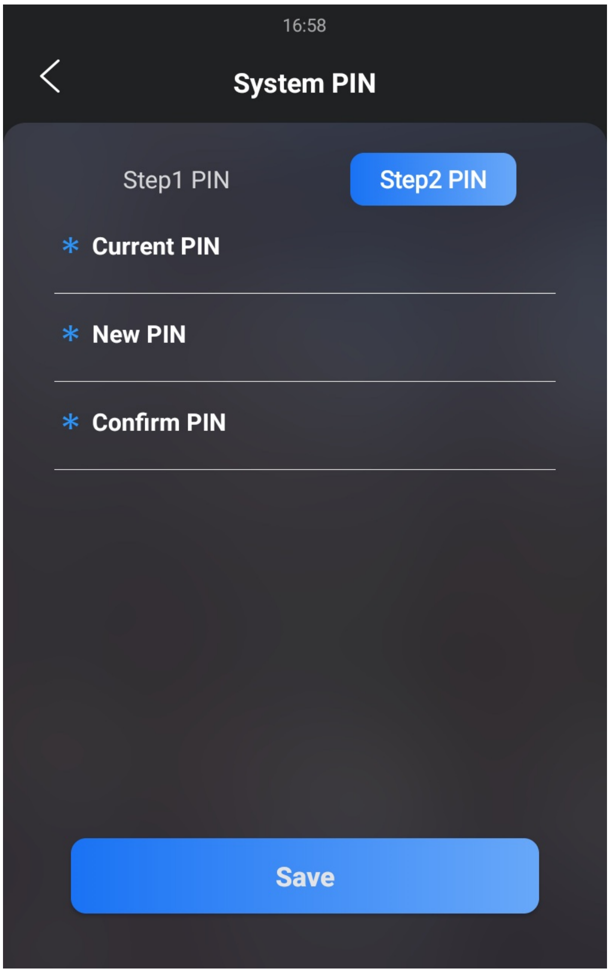
Note

- The default system entry password is 9999 and the system setting password is 3888.

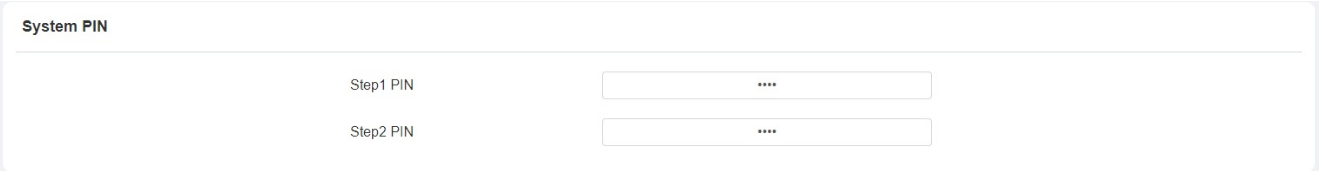
Modify Setting Password

Setting PIN code is used to access the device setting. You can modify the system PIN code on the device and web interface.

To set the system PIN code on the device, go to **Security > System PIN**, then select **Step2 PIN**.



To set up the setting password on the web interface, navigate to **System > Security > System PIN.**


System PIN

Step1 PIN	••••
Step2 PIN	••••

Note

- The default system entry password is 9999 and the system setting password is 3888.

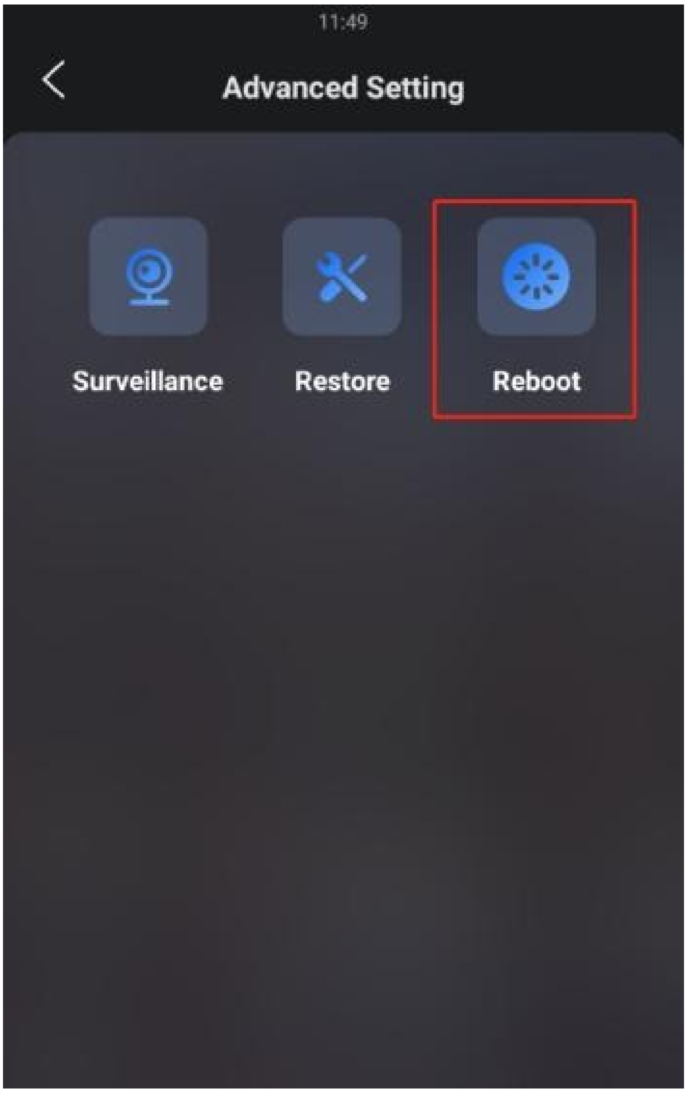
System Reboot&Reset

Reboot

To restart the system setting on the web **System > Upgrade** interface.

Reboot
Reboot

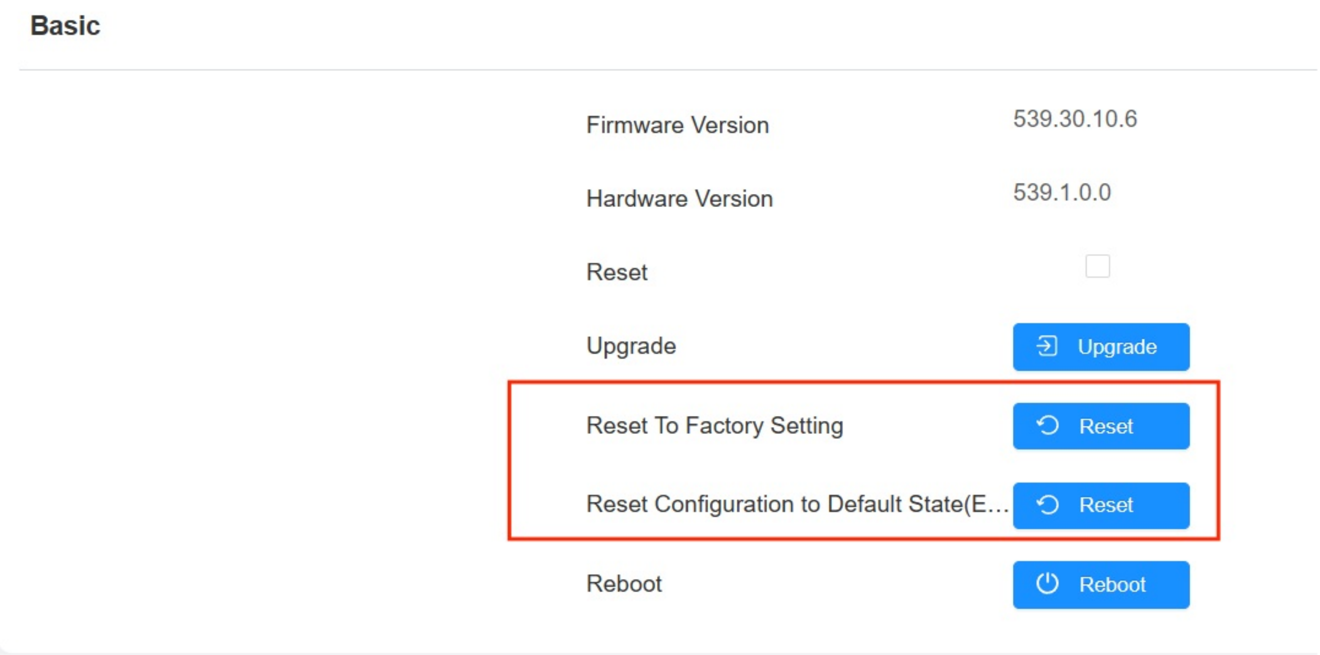
To reboot the device, go to **Advanced Setting > Reboot**.



Reset

You can select **Reset To Factory Setting** if you want to reset the device (deleting both configuration data and user data such as RF cards, face data, and so on). Or, select **Reset Configuration to Default State (Except Data) Reset**, if you want to reset the device (retaining the user data).

To reset the device, go to **System > Upgrade**.



Basic

Firmware Version 539.30.10.6

Hardware Version 539.1.0.0

Reset □

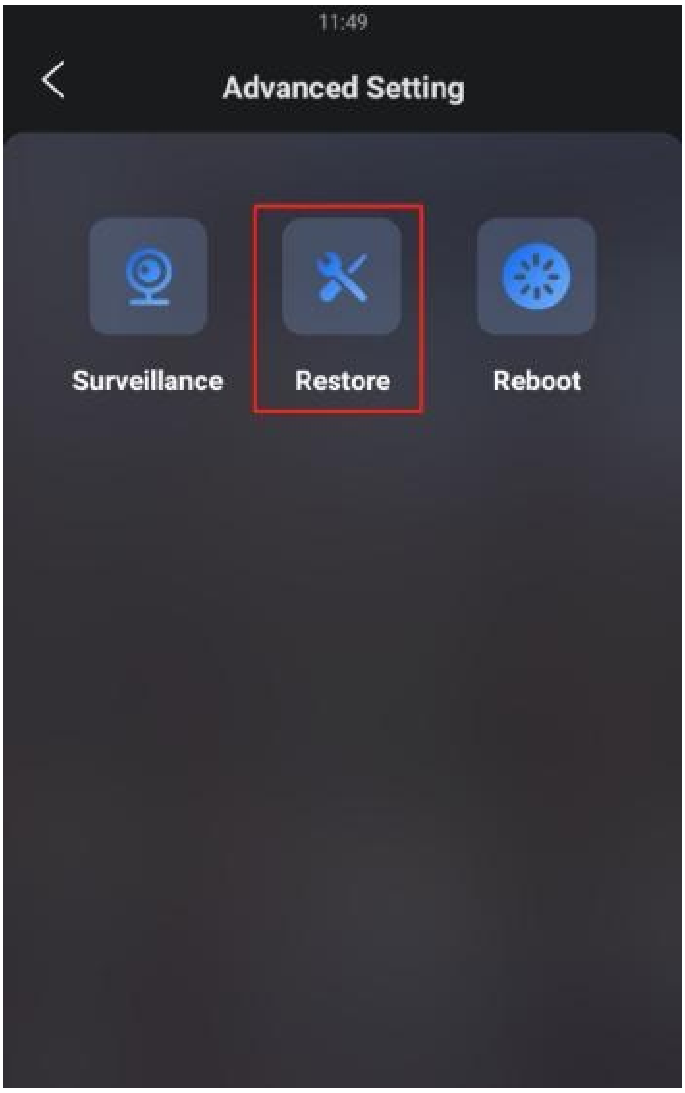
Upgrade

Reset To Factory Setting

Reset Configuration to Default State(E…

Reboot

To reset the device to the factory setting on the device, go to **Advanced Setting > Restore**.


11:49
Advanced Setting
Surveillance
Restore
Reboot