About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM

AKUVOX E18C DOOR PHONE

Administrator Guide

Thank you for choosing Akuvox E18C door phone. This manual is intended for administrators who need to properly configure the door phone. This manual applies to the 18.30.10.8 version, and it provides all the configurations for the functions and features of E18C door phones. Please visit Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

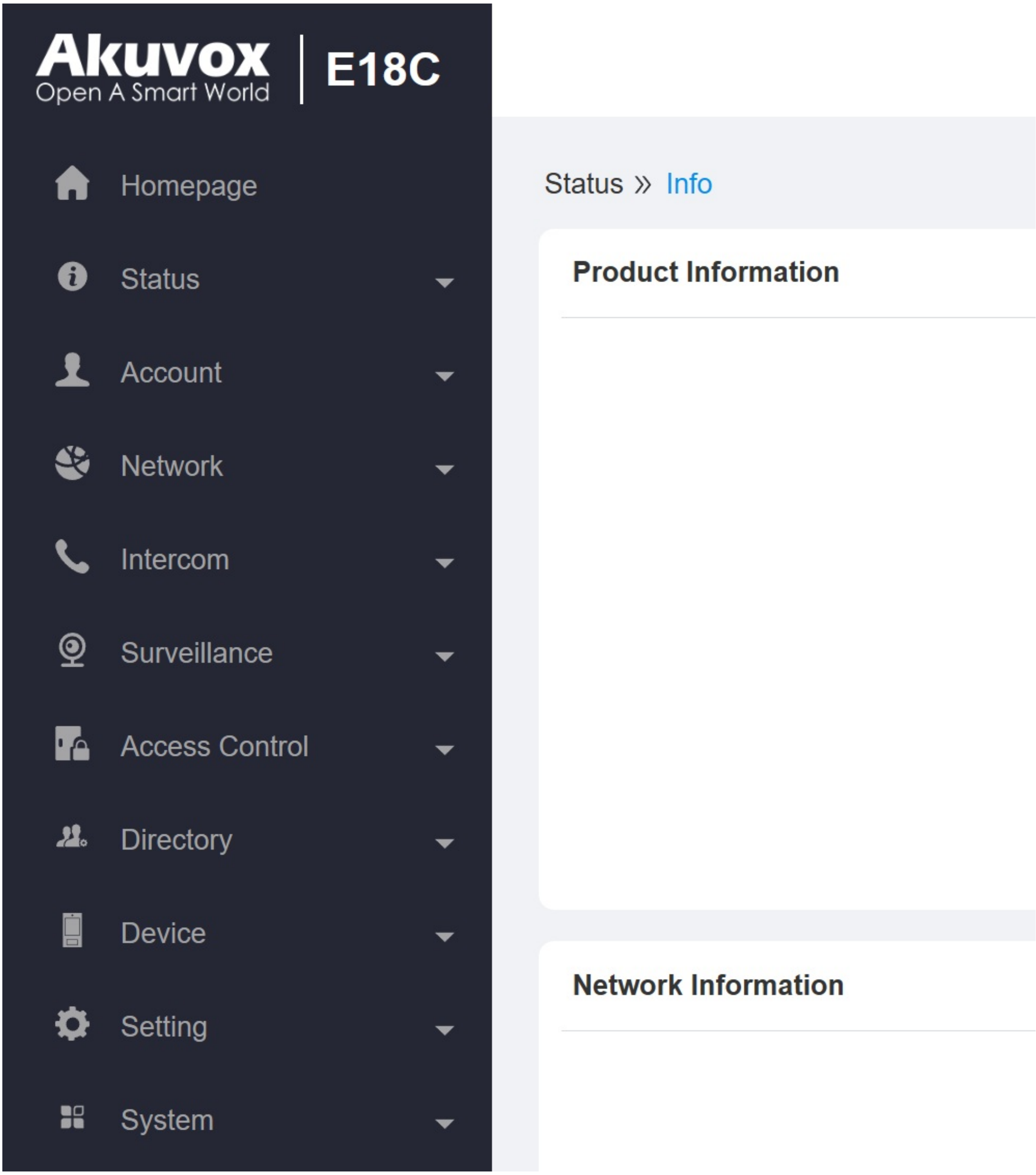
Akuvox E18C is Linux-based with a touch screen. It incorporates audio and video communications, access control, and video surveillance. Its finely-tuned SmartPlus and AI-based communication technology allow featured customization to better suit your operation habit. E18C multiple ports, such as RS485 and Wiegand ports, can be used to easily integrate external digital systems, such as elevator controller and fire alarm detector, 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 door access in an accompaniment with body temperature measurement. E18C door phone applies to residential buildings, office buildings, and their complex.

Model Specification

Model	E18C
Relay Out	2
Relay In	3
RS485	✔
Card Reader	13.56MHz, 125kHz & NFC
Wi-Fi	X
Bluetooth	✔
Temperature Detection	Optional
Face Recognition	✔
LTE	Optional
USB	X
External SD Card	✔

Introduction to Configuration Menu

- **Status**: this section gives you basic information such as product information, Network Information, and account information, call log, access log, and temperature log.
- **Account**: this section concerns SIP account, SIP server, proxy server, transport protocol type, outbound proximity server.
- **Network**: this section mainly deals with DHCP&Static IP settings, and device deployment etc.
- **Intercom**: this section covers intercom call setting, call features, dial plan and so on.
- **Surveillance**: this section includes audio&video related settings such as Live stream, RTSP, ONVIF, MJPEG.
- **Access Control**: this section includes input type setting, relay setting, web relay setting, private PIN code, facial recognition, RF card, BLE setting, and body temperature and so on.
- **Directory**: this section allows you to add users and configure user-specific door access control. It also lets you set up contact groups and contacts are displayed on the door phone.
- **Device**: this section concerns LED light, Wiegand, lift control, LCD display and audio and so on.
- **Setting**: this second deals with time, language, security notification settings, door prompt text setting, action URL, schedule, and HTTP API and so on.
- **System**: this section covers Firmware upgrade, device reset&reboot, configuration file auto-provisioning, PCAP password modification, tamper alarm, and web interface automatic logout.

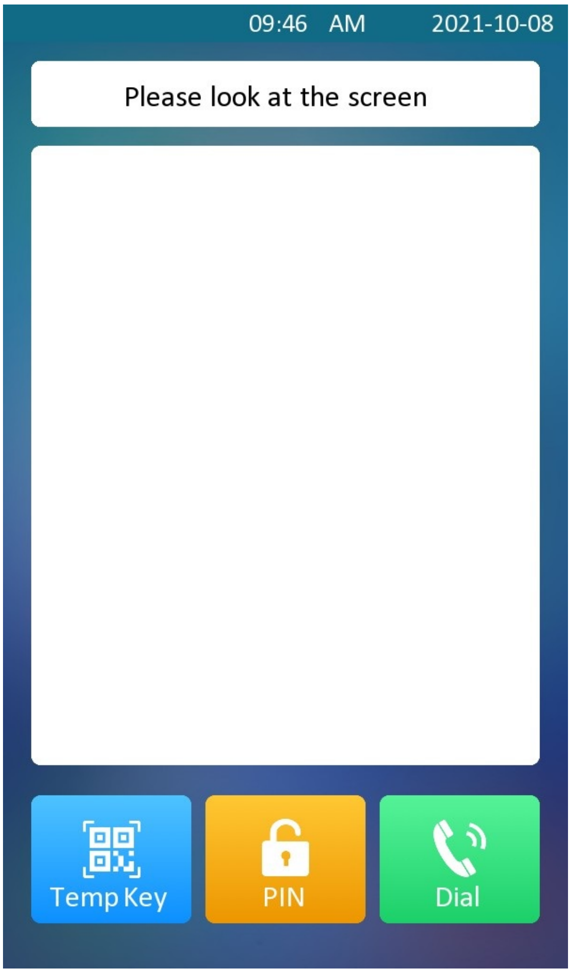

Akuvox
Open A Smart World
E18C
Homepage
Status
Account
Network
Intercom
Surveillance
Access Control
Directory
Device
Setting
System
Status » Info
Product Information
Network Information

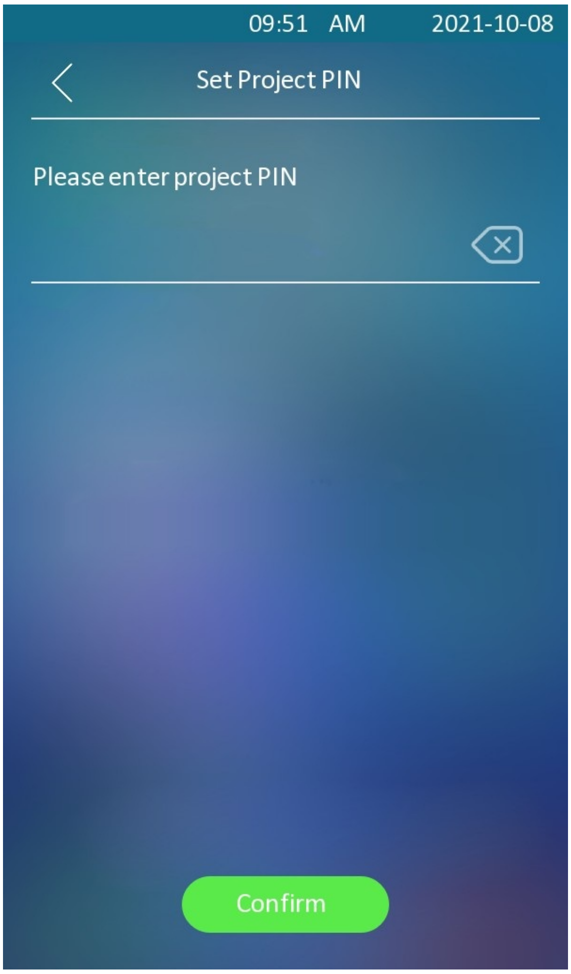
Access the Device

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

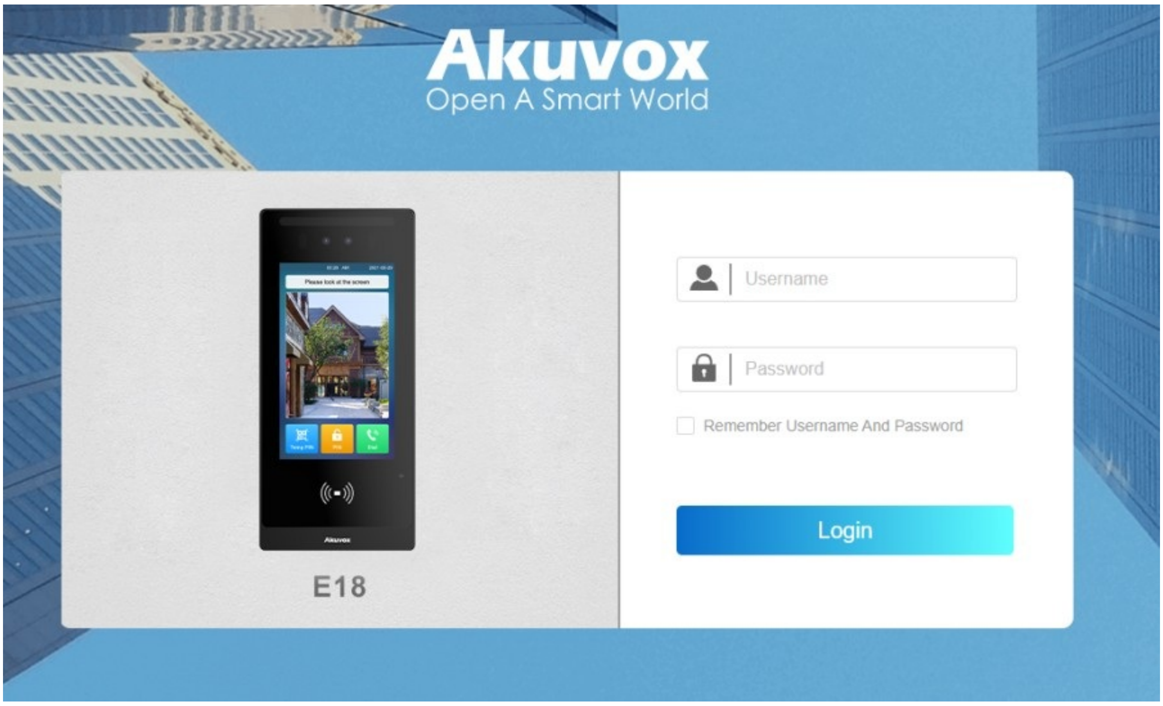
If you want to access the device setting to configure and adjust the parameters, you can do it directly on the device. You can press anywhere on the initial screen for approximately five seconds, enter the default PIN code **admin**, then press **Confirm** tab.





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.
- Download IP scanner: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- See 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.

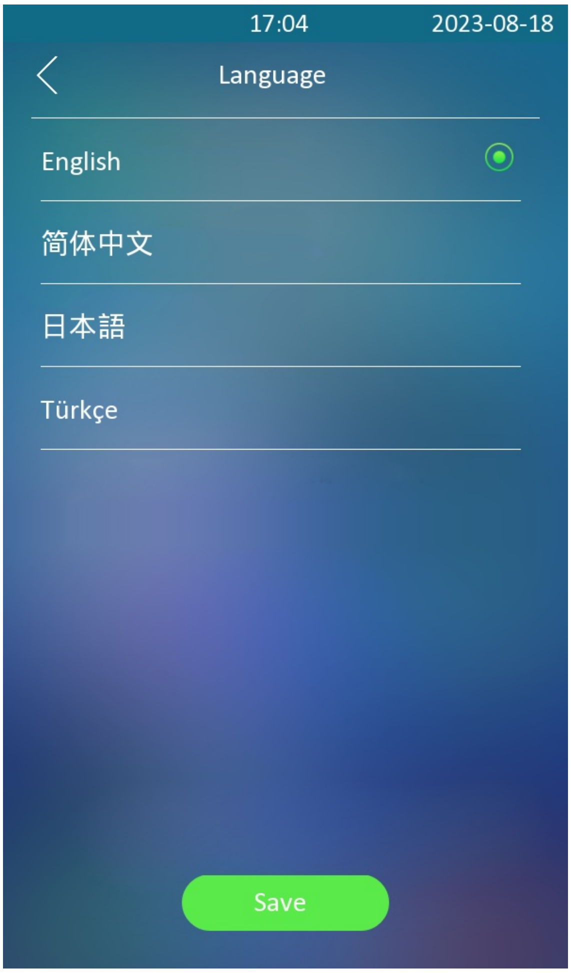
Time and Language Setting

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

Device Language can be configured on the device and on the device web interface that allows you to select or change the language for screen display to your preference. Path: **Display&Sounds > Language.**



English ●

简体中文

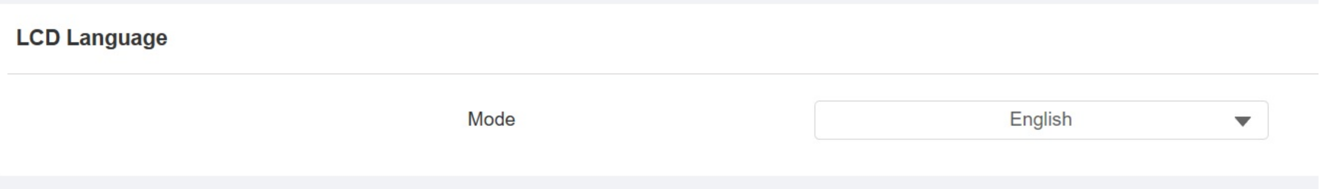
日本語

Türkçe

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.

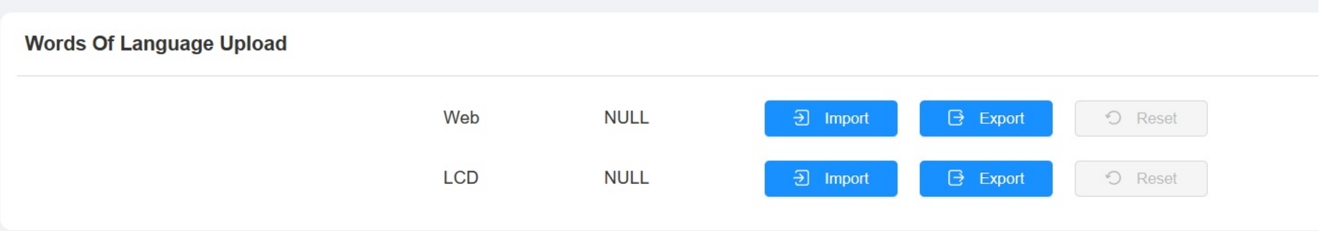
Navigate to **Setting >Time/Lang > LCD Language.**



LCD Language

Mode: English

To customize configuration names and prompt text, you need to export and edit the .json file before uploading the file to the device. Path: **Setting > Time/Lang > Words Of Language Upload.**



Words Of Language Upload

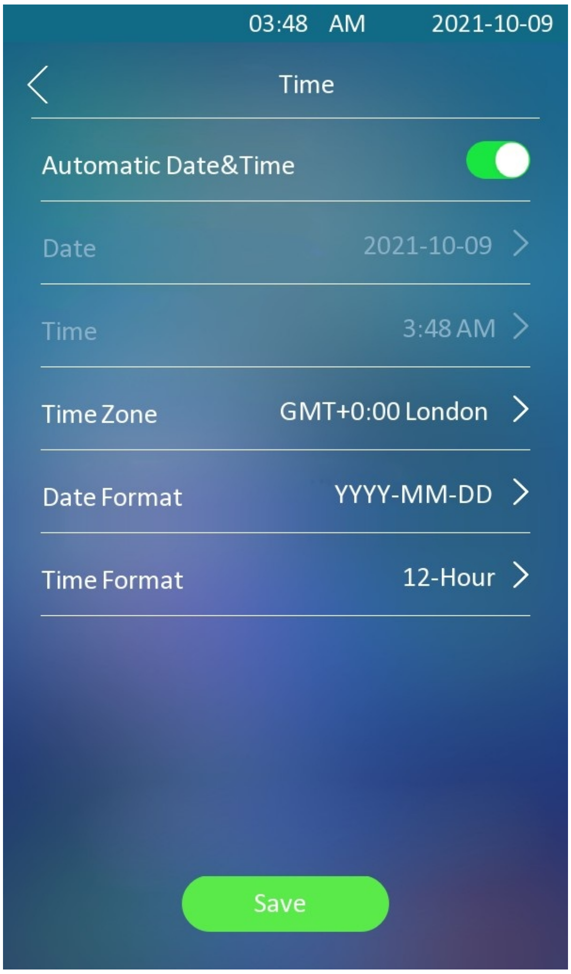
Web	NULL	Import	Export	Reset
LCD	NULL	Import	Export	Reset

Time Setting

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

Configure Time Setting on the Device

Path: **Display&Sounds > Time.**



03:48 AM 2021-10-09

Time

Automatic Date&Time ●

Date 2021-10-09 >

Time 3:48 AM >

Time Zone GMT+0:00 London >

Date Format YYYY-MM-DD >

Time Format 12-Hour >

Save

Parameter Set-up:

- **Automatic Date&Time**: Automatic Date&Time 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, then entering the time and date you want before pressing the **Save** tab for the validation.

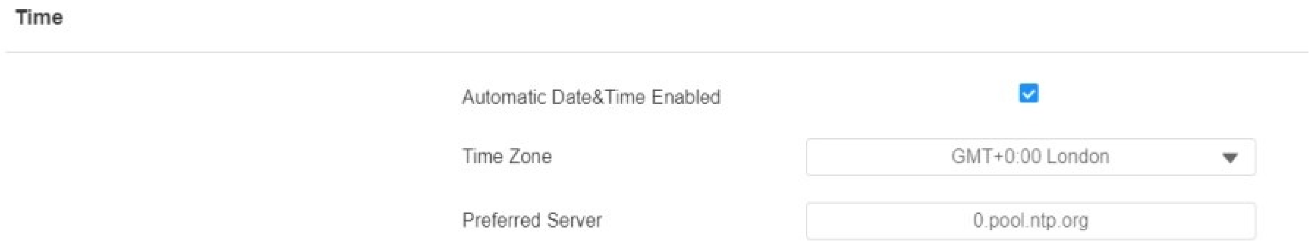
Note

- When the **Automatic Date&Time** toggle switch is toggled off then parameters related to the NTP server will become not editable. And when the switch is toggled on, the 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.

Navigate to **Setting > Time/Lang** interface.



Time

Automatic Date&Time Enabled ☑

Time Zone: GMT+0:00 London

Preferred Server: 0.pool.ntp.org

Parameter Set-up:

- **Automatic Date&Time Enabled**: tick the checkbox to allow the date& time in the device to be automatically set up and synchronized with the default time zone and the NTP server (**Network Time Protocol**). If you untick the checkbox, then you are allowed to set up the time manually on the web interface.
- **Preferred Server**: enter the NTP server you obtained in the NTP Server field.

Note

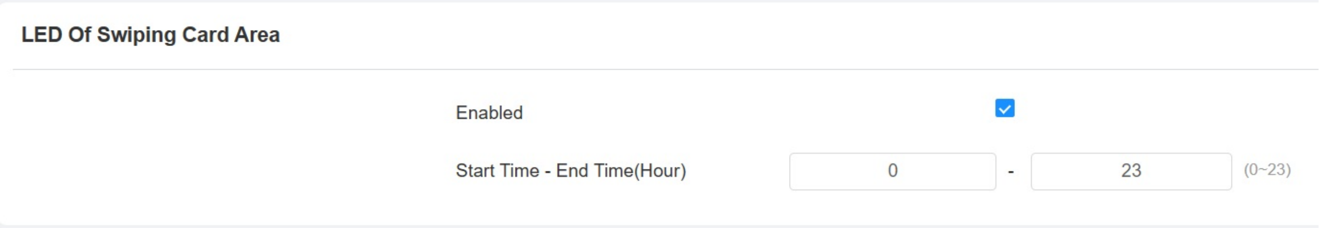
- When the check box is unticked, the parameters related to the NTP server will become uneditable.

LED & LCD Setting

Configure Card Reader LED Setting

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.

Path: **Device > Light > LED of Swiping Card Area**.



LED Of Swiping Card Area

Enabled ☑

Start Time - End Time(Hour) 0 - 23 (0~23)

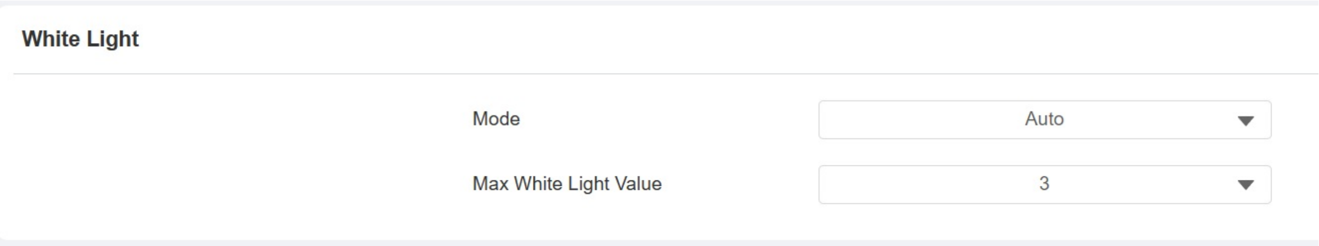
Parameter Set-up:

- **Start Time - End Time (H)**: enter the time span for the LED lighting to be valid, e.g. if the time span is from **18-22** it means the LED light will stay on during the time span from **6:00 pm** to **10:00 pm** during one day (24 hours).

Configure 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.

Path: **Device > Light > White Light.**



White Light

Mode: Auto

Max White Light Value: 3

Parameter Set-up:

- **Mode**: select **Auto** or **OFF**. If you select Auto then the white light will turn on for 5 minutes for facial recognition and QR code scan. And if you select **Off** then the white light will be turned off.

- **Max White Light Value**: set the white light value from **1-5**, and the default white light value is 3. The greater value it is, the brighter the light will be.

Note

- IR LED light should be triggered first before the white light can be valid in the facial recognition, however, IR LED light does not need to be triggered for the white light function in the QR code scan.

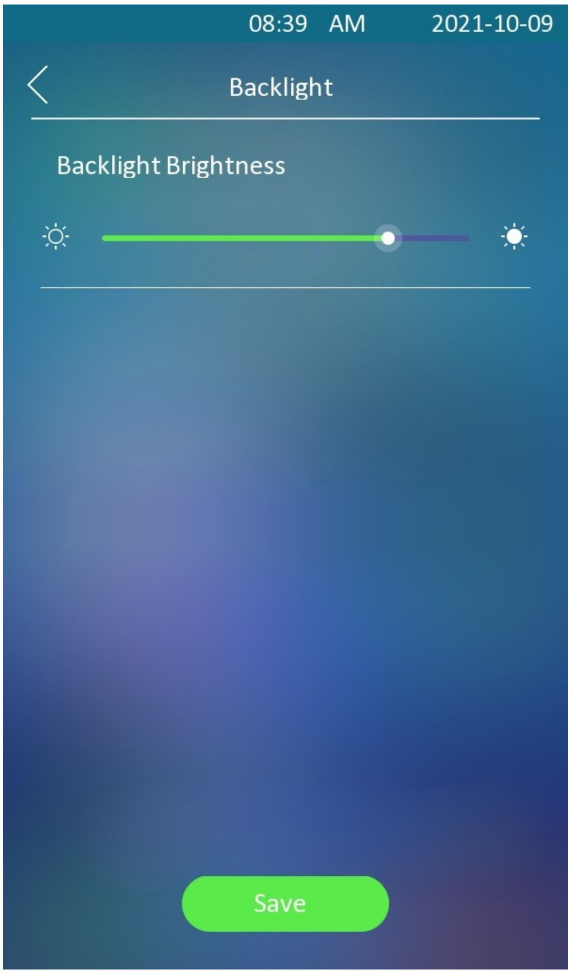
LCD Screen Brightness Setting

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 Device

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

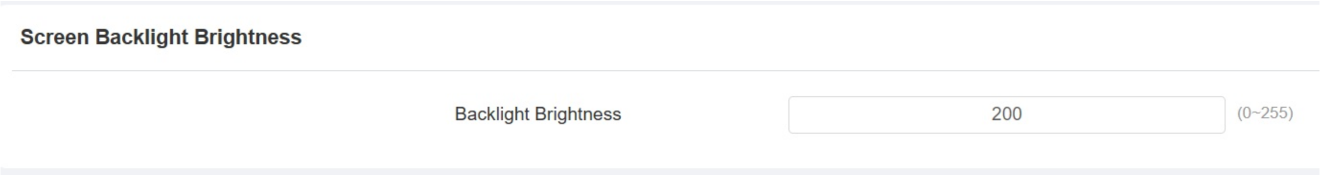
Path: **Display&Sounds > Backlight.**



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.

Path: **Device > Light > Screen Backlight Brightness.**



Screen Backlight Brightness

Backlight Brightness: 200 (0~255)

Parameter Set-up:

- **Backlight Brightness (day)**: set the screen backlight brightness during the daytime with the value ranging from (0-255).

Screen Display Configuration

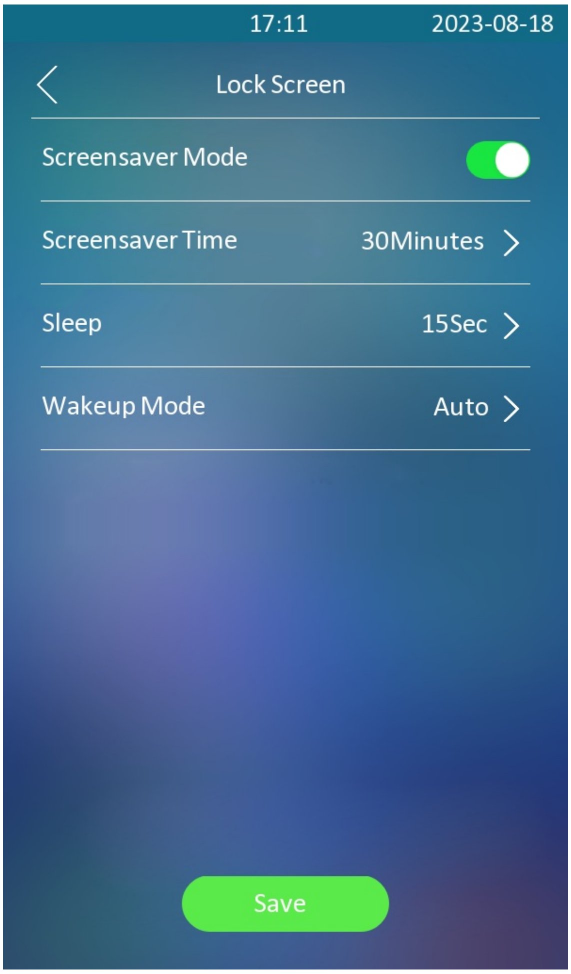
You can set up the device's screen display features such as screensaver to give users a better visual and operational experience.

Configure Screensaver

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.

Path: **Display&Sounds > Screensaver > Lock Screen.**



17:11 2023-08-18

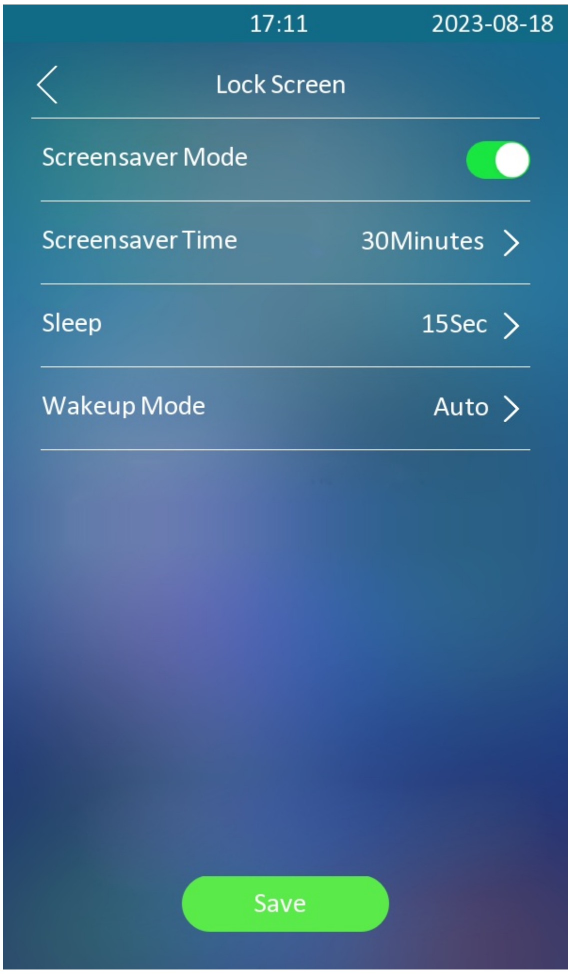
Lock Screen

Screensaver Mode: on

Screensaver Time: 30Minutes

Sleep: 15Sec

Wakeup Mode: Auto


17:11 2023-08-18

Lock Screen

Screensaver Mode

Screensaver Time 30Minutes

Sleep 15Sec

Wakeup Mode Auto

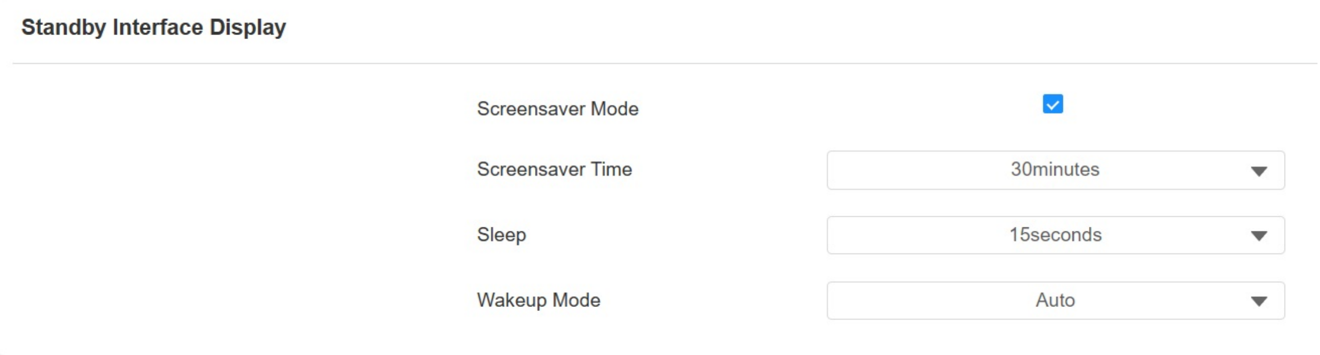
Parameter Set-up:

- **Screensaver Mode**: move the toggle switch to the right to enable the screen saver function.
- **Screensaver Time**: set the screensaver duration after the device goes into sleep mode. The default setting is 30 min.
- **Sleep**: select the time from **5 sec, 10 sec**, and **15 sec.** For example, if you set it as 10 sec, then the device will go into screen saver mode in 10 sec when there is no operation on the device or no one is detected approaching.
- **Wakeup Mode**: if you select **Auto** mode, then the screen will be awakened when someone approaches without it being touched upon, and if **Manual** mode is selected, then you have to touch and wake up the screen.

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 screensaver on the web interface, you can go to **Device > LCD > Standby Interface Display**.



Standby Interface Display

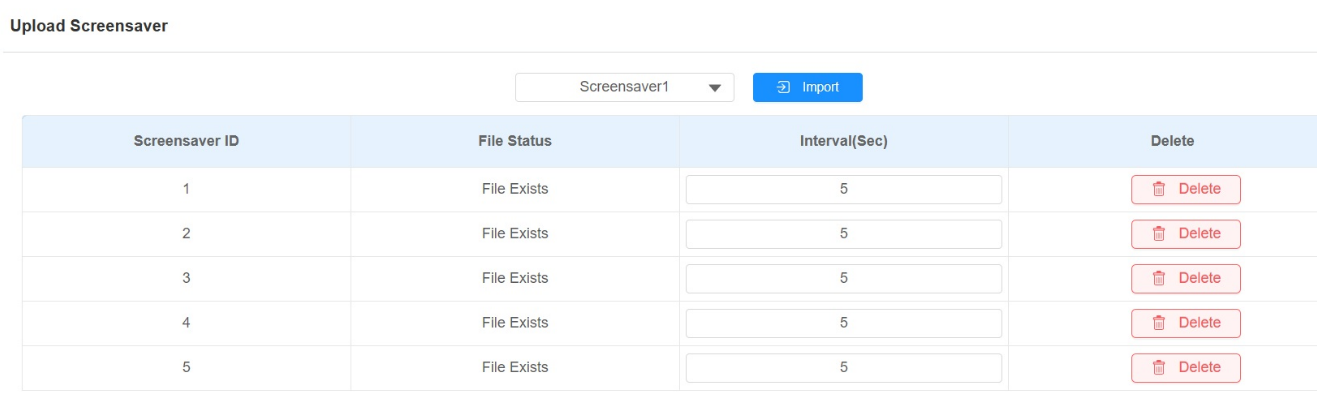
Screensaver Mode	☑
Screensaver Time	30minutes
Sleep	15seconds
Wakeup Mode	Auto

Parameter Set-up:

- **Screensaver Time**: set the screensaver duration after the device goes into sleep mode. Screensaver duration ranges from **5 seconds** to **2 hours** on the web interface. The default setting is **30 min.**
- **Sleep**: select the time from **5 sec, 10 sec**, and **15 sec**. For example, if you set it as 10 sec, then the device will go into screen saver mode in 10 sec when there is no operation on the device or no one is detected approaching.
- **Wakeup Mode**: if you select **Auto** mode, then the screen will be awakened when someone approaches without it being touched upon, and if **Manual** mode is selected, then you have to touch and wake up the screen.

Customize Screensaver on the Web Interface

You can upload and customize screensaver pictures separately or in batch to the device for public purposes or for a greater visual experience. You are allowed to upload a maximum of 5 pictures, and each picture will be displayed in rotation according to the ID order with the specific time duration (Time Interval) you set. You can go to **Device > LCD > Upload Screensaver**.



Upload Screensaver

Screensaver1 Import

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

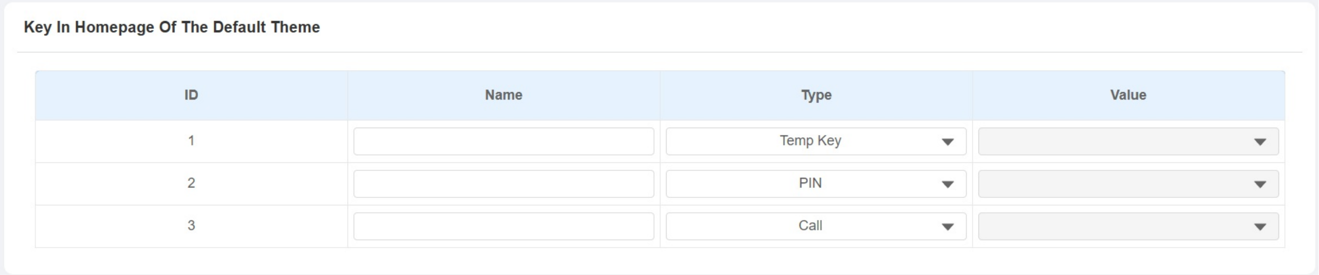
Parameter Set-up:

- **Interval(Sec)**: set the display time of each picture you uploaded in **Interval (Sec.)**. The display time range is from **1-120** seconds. The default setting is 5 seconds.

> **Note**
>
> - The pictures uploaded should be in **JPG format** with 2M pixel maximum.

Home Screen Configuration

You can change the home screen display through the configuration of tab name and tab arrangement on the device web interface if needed. Path: **Device > LCD > Key In Homepage Of The Building Theme.**



Key In Homepage Of The Default Theme

ID	Name	Type	Value
1		Temp Key	
2		PIN	
3		Call	

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 **Speed Dial** tab to be displayed in position one, you can change the type in index number 1 to **Speed Dial**. And you can change another tab position accordingly.
- **Name**: enter a new name to replace the original type of name, but it does not change the attribute of the type.
- **Value**: enter the IP or SIP number to be attached to the reception icon for the speed dial. The number entered will be dialed out as you press the reception icon on the home screen. This field is only valid for speed dial.

Volume & 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.

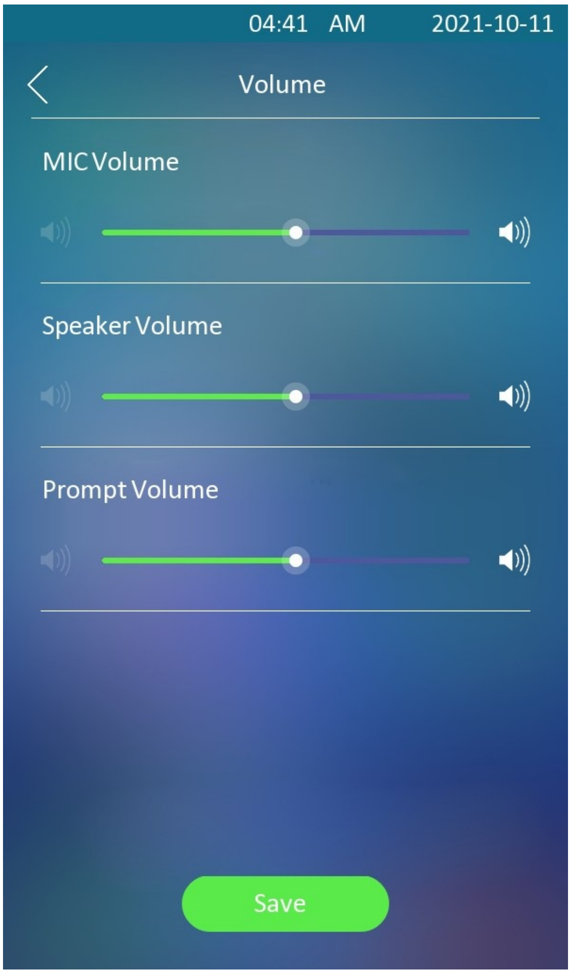
Volume Configuration

You can configure the Mic volume according to your need for open-door notification. Moreover, you can also set up the tamper alarm volume when unwanted removal of the access control terminal occurs.

Configure Volume on the Device

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

Path: **Display&Sounds > Sounds.**



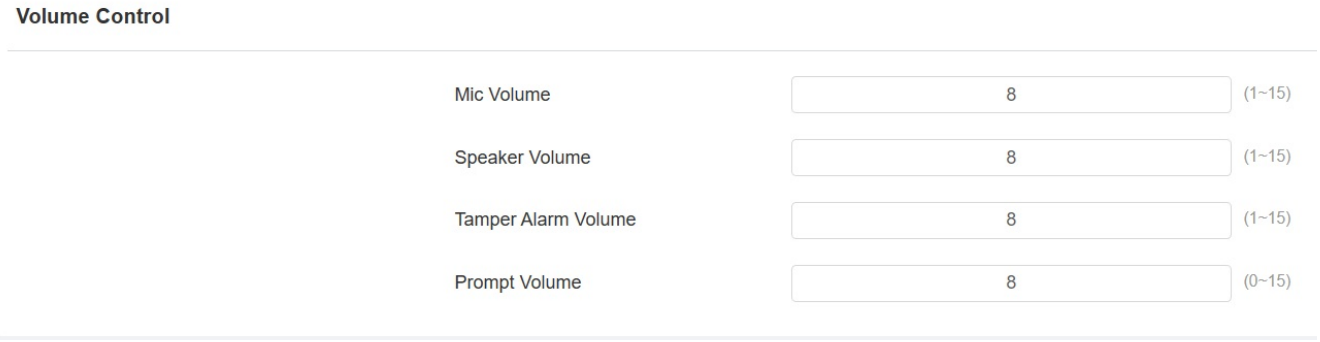
Parameter Set-up:

- **Prompt Volume**: adjust the prompt volume, which includes various types of prompt sounds for door open success and failure, ringback, temperature measurement sound, etc.

Configure Volume on the Web Interface

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

Path: **Device > Audio > Volume Control.**



Volume Control

Mic Volume	8	(1~15)
Speaker Volume	8	(1~15)
Tamper Alarm Volume	8	(1~15)
Prompt Volume	8	(0~15)

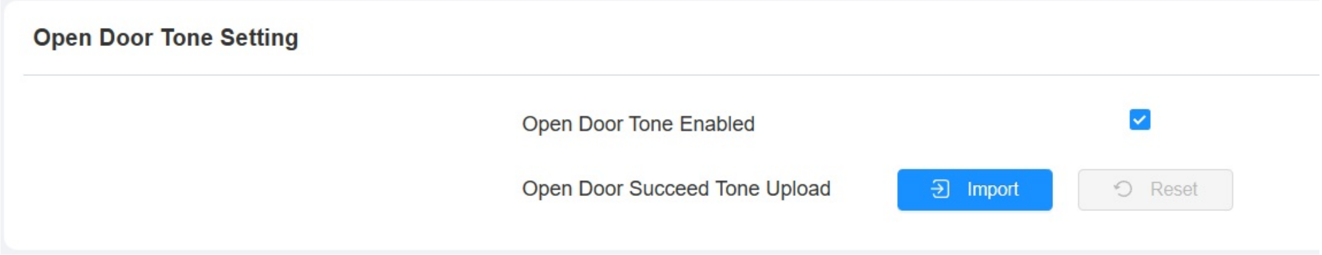
Parameter Set-up:

- **Prompt Volume:** adjust the prompt volume, which includes various types of prompt sounds for door open success and failure, ringback, temperature measurement sound, etc.

Upload Open Door Tone

You can upload the tone for open door failure and success on the device web interface.

Path: **Device >Audio > Open Door Tone Setting.**



Open Door Tone Setting

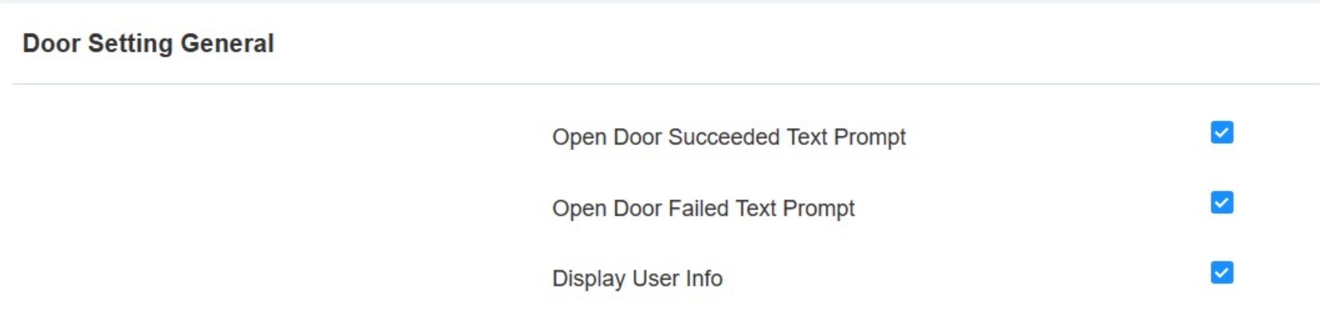
Open Door Tone Enabled ☑

Open Door Succeed Tone Upload

Configure Door Open Prompt Text

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.

Path: **Access Control > Relay > Door Setting General.**



Door Setting General

Open Door Succeeded Text Prompt ☑

Open Door Failed Text Prompt ☑

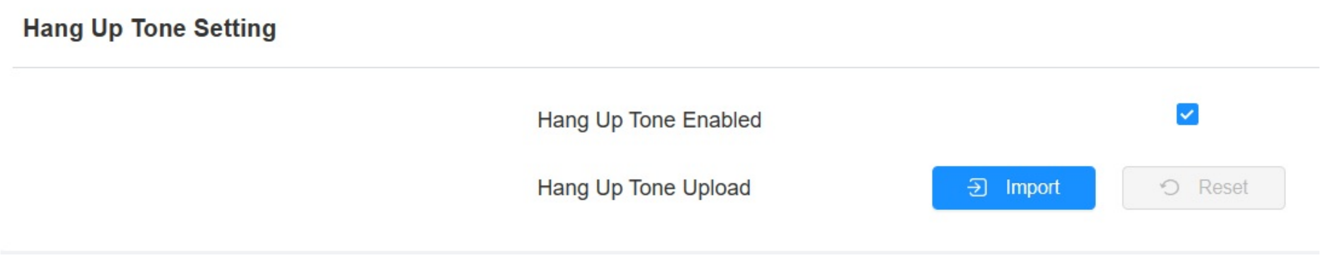
Display User Info ☑

Parameter Set-up:

- **Open Door Succeeded Text Prompt**: tick the check box if you want to see the text prompt after the door open success and vice versa.
- **Open Door Failed Text Prompt**: tick the check box if you want to see the prompt words after the door open failure and vice versa.

Configure Hang-up Tone

You can customize your call hang-up tone if needed. Path: **Device > Audio > Hang Up Tone Setting.**



Hang Up Tone Setting

Hang Up Tone Enabled ☑

Hang Up Tone Upload

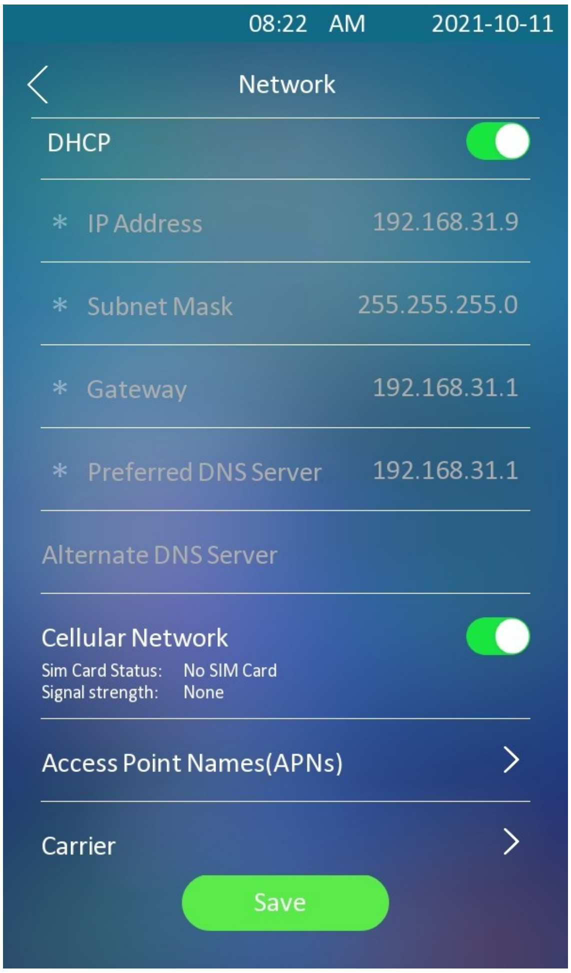
Parameter Set-up:

- **Hang Up Tone Upload**: upload the hang-up tone file in .wav format. And the file size shall be less than 200KB. You can click on **Reset** if you want to delete the uploaded file and then change it back to the default hang-up tone.

Network Setting

Device Network Connection Setting

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



08:22 AM 2021-10-11

Network

DHCP ●

* IP Address 192.168.31.9

* Subnet Mask 255.255.255.0

* Gateway 192.168.31.1

* Preferred DNS Server 192.168.31.1

Alternate DNS Server

Cellular Network ●

Sim Card Status: No SIM Card

Signal strength: None

Access Point Names(APNs) >

Carrier >

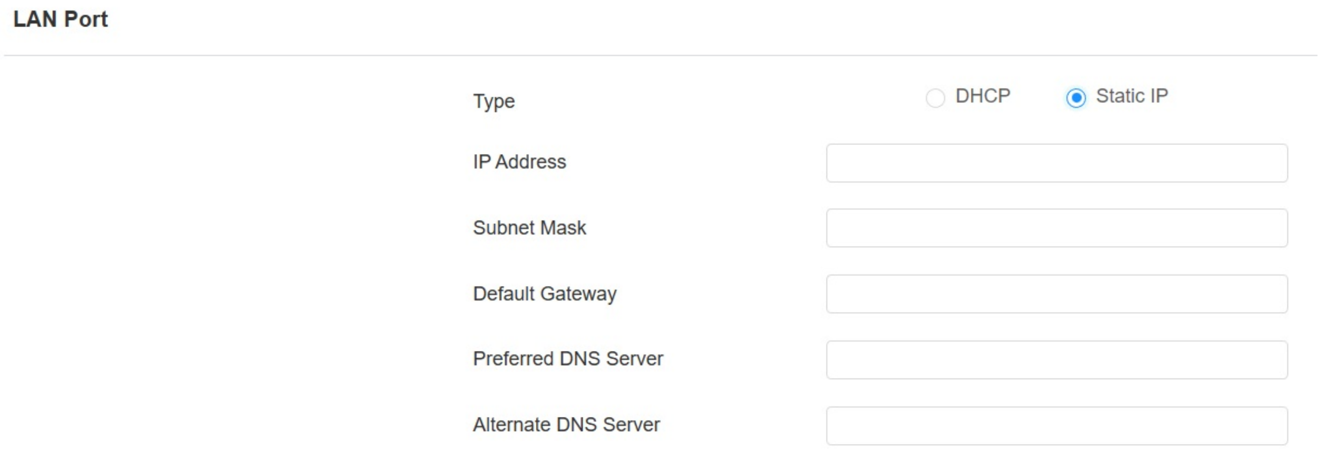
Save

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 IP address, subnet mask, default gateway, and DNS server address automatically.
- **Static IP**: When static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS servers 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 an alternate DNS Server (**Domain Name Server**) according to your actual network environment. 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.

You can also configure the network work setting on the web interface. Path: **Network > Basic > LAN Port.**



LAN Port

Type ○ DHCP ● Static IP

IP Address

Subnet Mask

Default Gateway

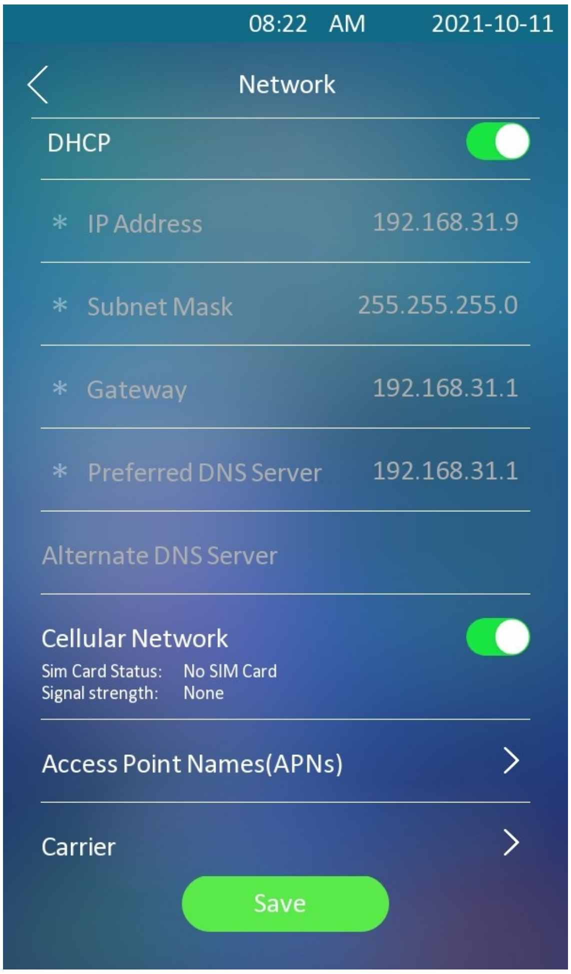
Preferred DNS Server

Alternate DNS Server

LTE Wireless Connection Setting

The LTE module enables cellular network connectivity for the device in areas where wired networks are unavailable, particularly beneficial for installations in older buildings.

Path: **Network > Cellular Network.**



08:22 AM 2021-10-11

Network

DHCP

* IP Address 192.168.31.9

* Subnet Mask 255.255.255.0

* Gateway 192.168.31.1

* Preferred DNS Server 192.168.31.1

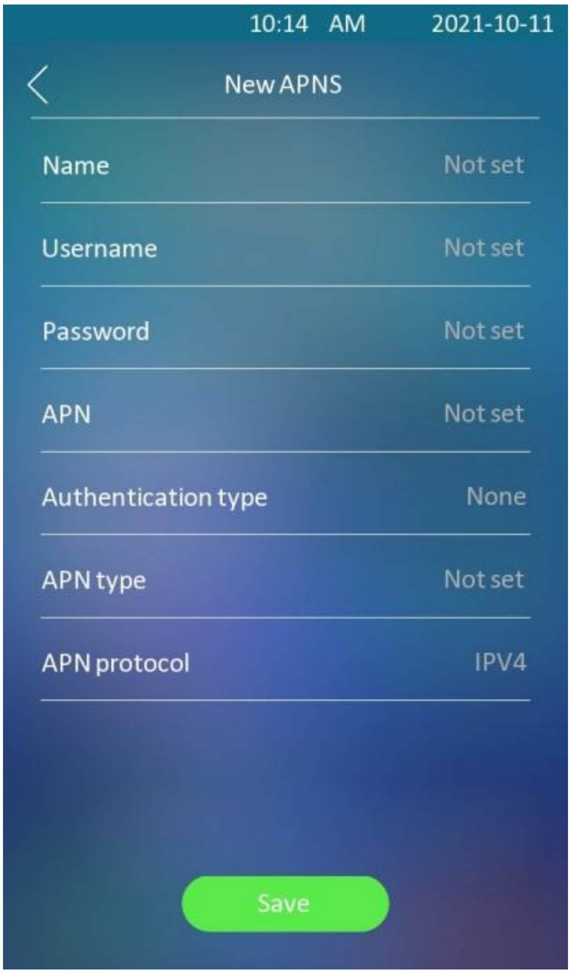
Alternate DNS Server

Cellular Network
Sim Card Status: No SIM Card
Signal strength: None

Access Point Names(APNs)

Carrier

Save



10:14 AM 2021-10-11

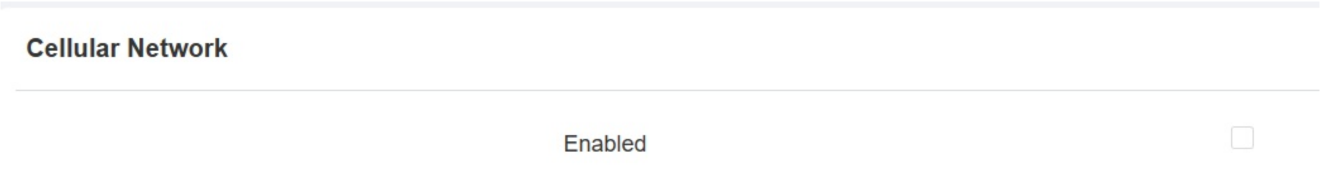
New APNS

Name	Not set
Username	Not set
Password	Not set
APN	Not set
Authentication type	None
APN type	Not set
APN protocol	IPV4

Parameter Set-up:

- **Cellular Network**: move the toggle switch on and off to enable or disable the LTE function. The signal strength has four levels: Weak, Fair, Good, and Excellent.
- **Access Point Name (APNs)**: check the Cellular Network provider for the Access Point. You can also add and delete APNs manually if needed.
- **Carrier**: enable or disable the network provided by the network service provider.

You can also enable or disable the 4G cellular network. Path: **Network > Advanced > Cellular Network.**



Cellular Network

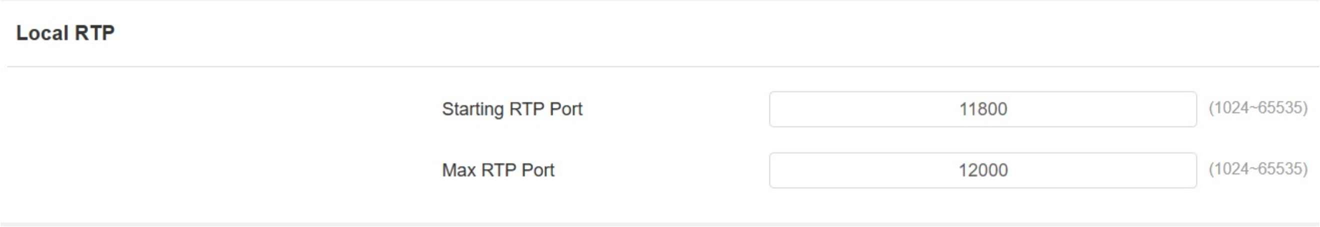
Enabled □

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.

Path: **Network > Advanced > Local RTP** interface.



Local RTP

Starting RTP Port: 11800 (1024~65535)

Max RTP Port: 12000 (1024~65535)

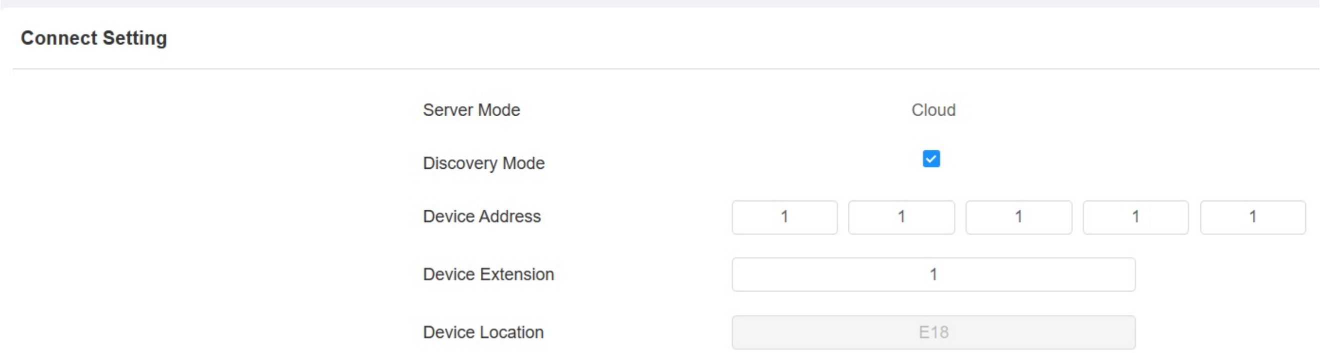
Parameter Set-up:

- **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.

Path: **Network > Advanced > Connect Setting.**



Connect Setting

Server Mode: Cloud

Discovery Mode: ☑

Device Address: 1 1 1 1 1

Device Extension: 1

Device Location: E18

Parameter Set-up:

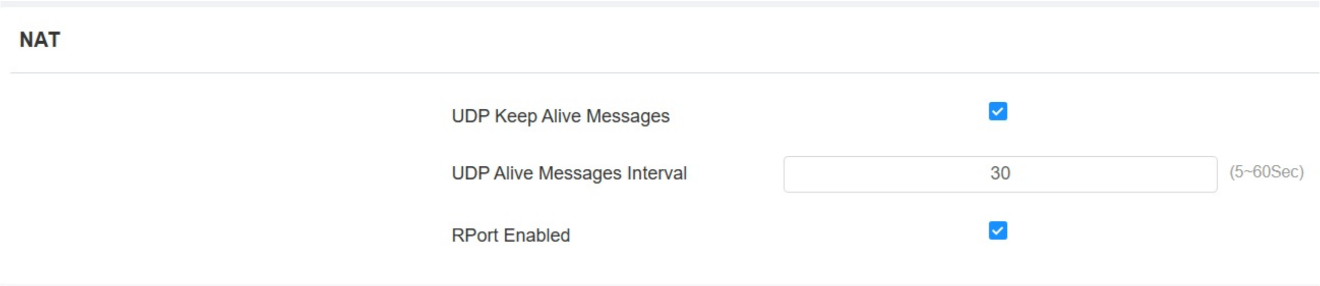
- **Server Mode**: it is automatically set up according to the actual device connection with a specific server in the network such as **SDMC** or **Cloud** and **None**. **None** is the default factory setting indicating the device is not in any server type. Therefore, you are allowed to choose **Cloud** or **SDMC** in discovery mode.

- **Discovery Mode**: click **Enabled** to turn on the discovery mode of the device so that it can be discovered by other devices in the network, and click **Disabled** if you want to conceal the device so as not to be discovered by other devices.
- **Device Node**: specify the device address by entering device location information from the left to the right: **Community, Unit, Stair, Floor**, and **Room** in sequence.
- **Device extension:** enter the device extension number for the device you installed.
- **Location**: enter the location in which the device is installed and used.

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.

Path: **Account > Advanced > NAT.**



NAT

UDP Keep Alive Messages ☑

UDP Alive Messages Interval 30 (5~60Sec)

RPort Enabled ☑

Parameter Set-up:

- **UDP Keep Alive Messages**: if enabled, the device will send out the message to the SIP server so that SIP server will recognize that 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**).

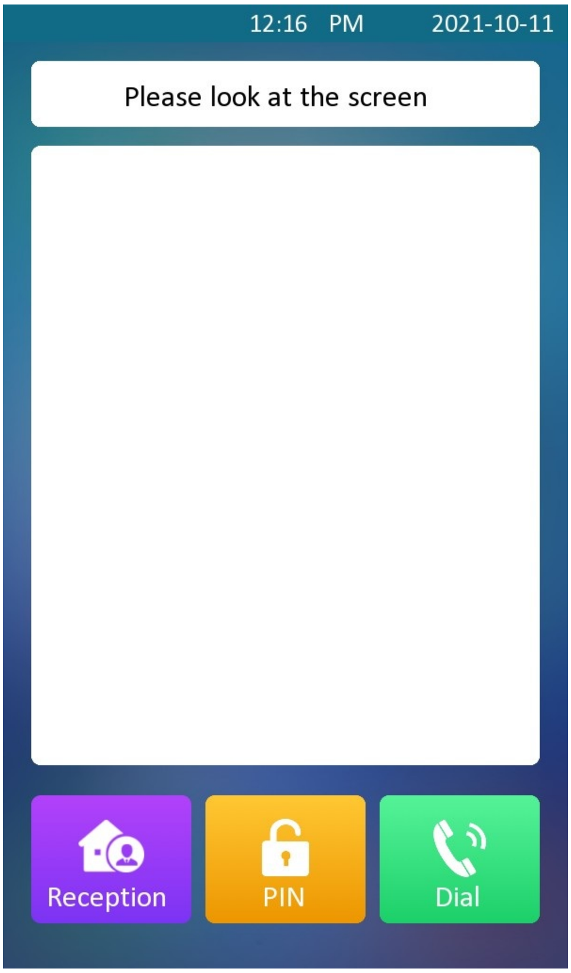
Intercom Call Configuration

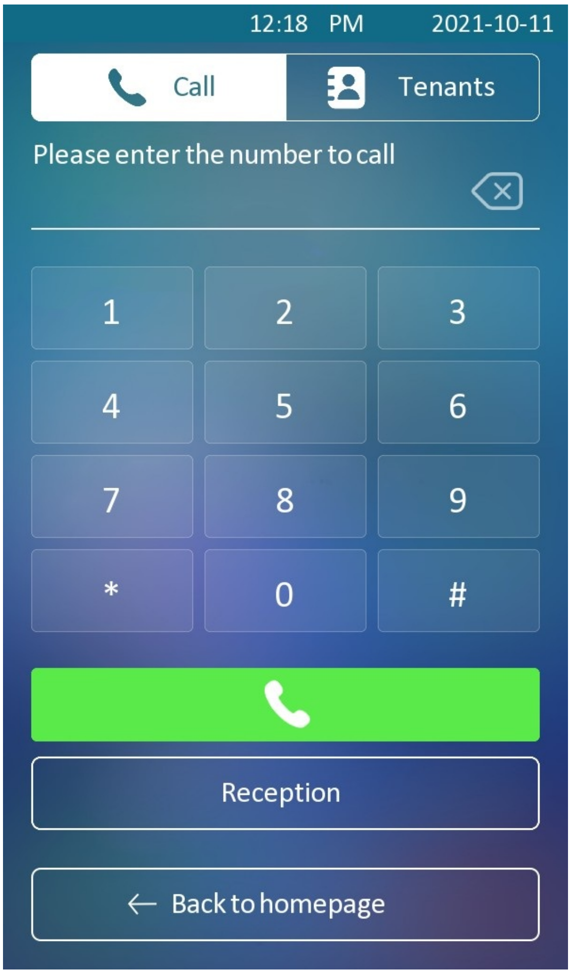
IP Call & IP Call Configuration

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/SIP calls

You can press the dial tab and make IP or SIP calls.

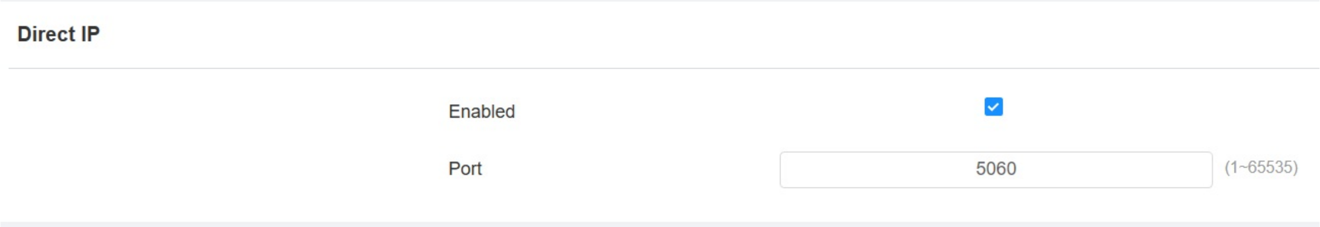




IP Call Configuration

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.

Path: **Intercom > Basic > Direct IP.**



Direct IP

Enabled ☑

Port 5060 (1~65535)

Parameter Set-up:

- **Enabled**: tick the checkbox to **Enable** or **Disable** the direct IP call. For example, if you do not allow direct IP calls to be made on the device, you can disable the function.
- **Direct IP Port**: the direct IP Port is **5060** by default with the port range from **1-65535.** If 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.

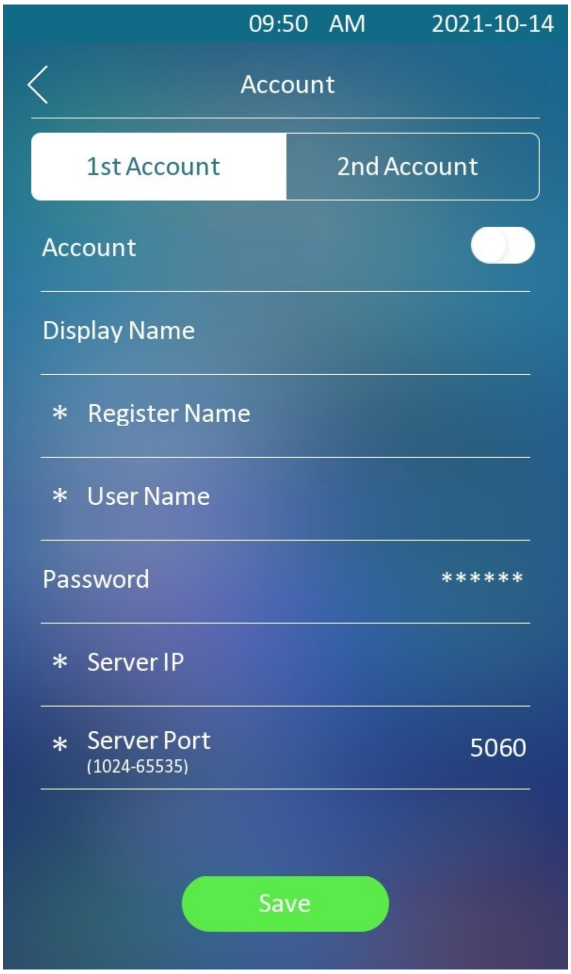
SIP Account Registration

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 SIP account on the device. Path: **Account**. **Register Name, User Name**, and **Password** are provided by the SIP account administrator.



09:50 AM 2021-10-14

Account

1st Account | 2nd Account

Account

Display Name

* Register Name

* User Name

Password ******

* Server IP

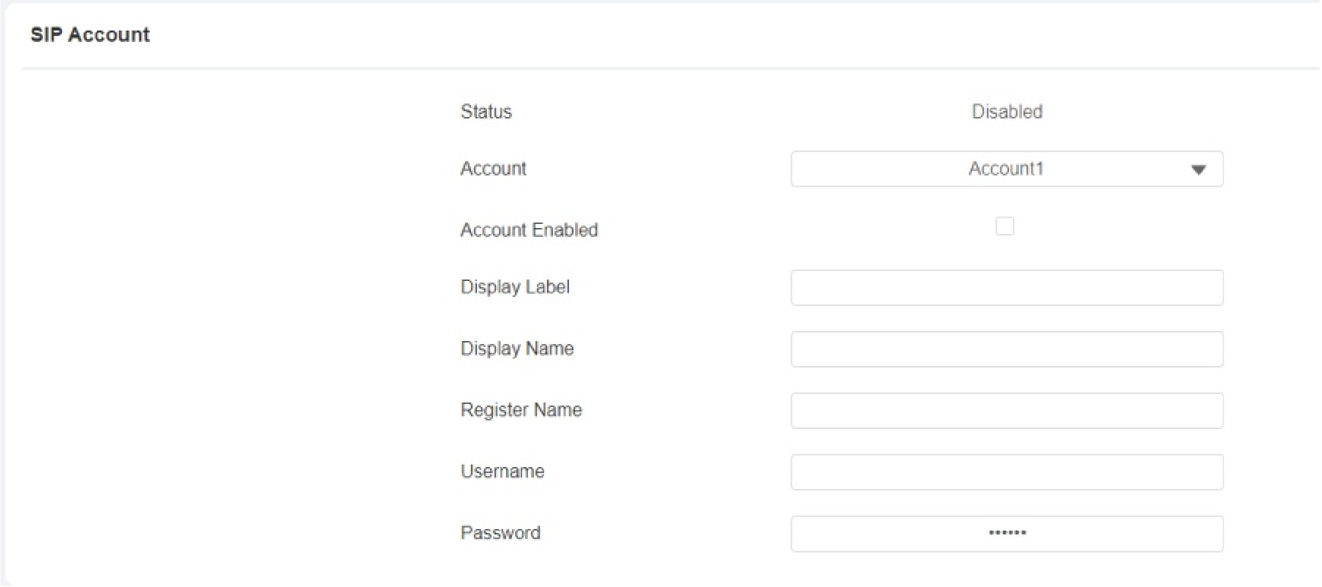
* Server Port (1024-65535) 5060

Parameter Set-up:

- **Display Name**: configure the name, for example, the device's name to be shown on the device being called to.
- **Server IP**: enter the SIP server address for the SIP account selected.
- **Server port**: enter the SIP server port for communication. The SIP port is 5060 by default.

Configure SIP Account on the Web Interface

To configure the configuration on the web interface, you go to **Account > Basic > SIP Account** interface. **Register Name, User Name**, and **Password** are provided by the SIP account administrator. You can fill in 63 bytes of characters in length maximum.



SIP Account

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

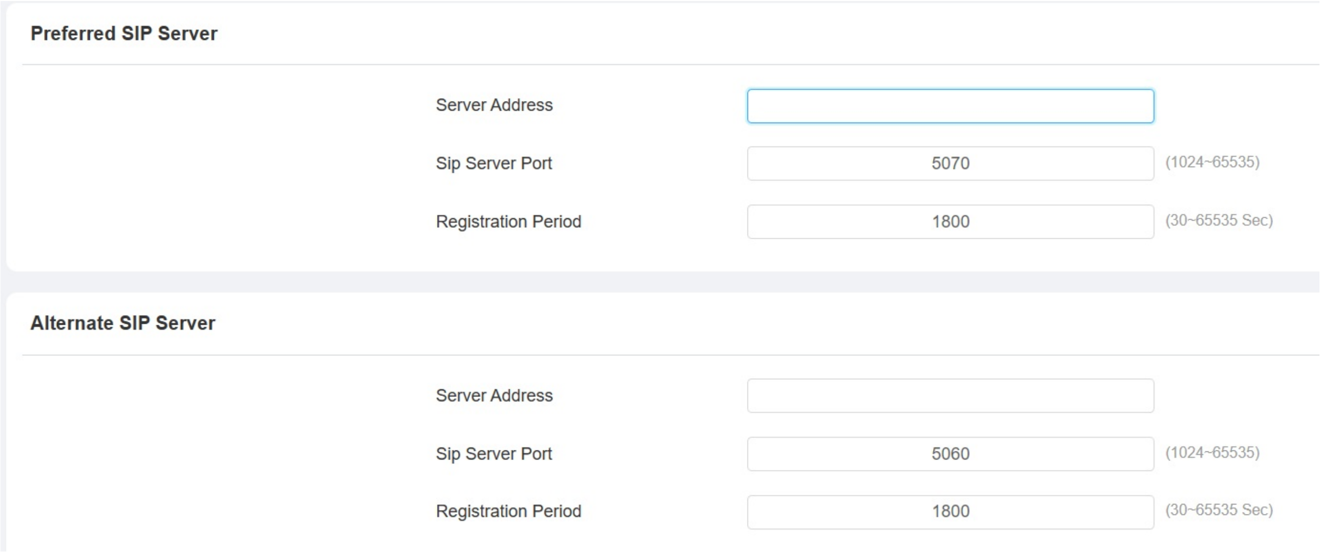
Parameter Set-up:

- **Status**: check to see if the SIP account is registered or not.
- **Account**: select the exact account (Account 1&2) to be configured.
- **Account Enabled**: tick the checkbox to enable or disable a registered SIP account.
- **Display Name**: configure the name, for example, the device's name to be shown on the device being called to. You can fill in 63 bytes of characters in length maximum.
- **Display Label**: configure the device label to be shown on the device screen. You can fill in 63 bytes of characters in length maximum.

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.

Path: **Account > Basic > Preferred SIP Server.**



Preferred SIP Server

Server Address		
Sip Server Port	5070	(1024~65535)
Registration Period	1800	(30~65535 Sec)

Alternate SIP Server

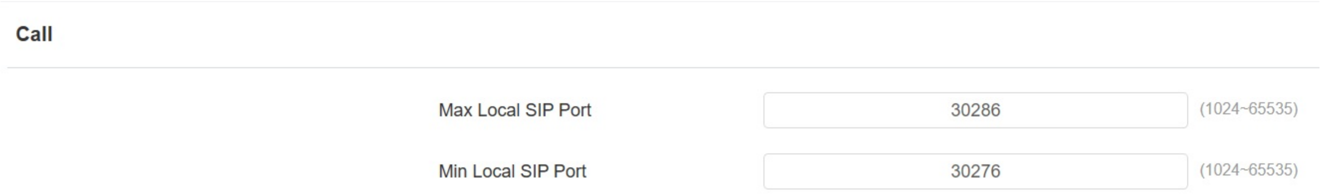
Server Address		
Sip Server Port	5060	(1024~65535)
Registration Period	1800	(30~65535 Sec)

Parameter Set-up:

- **Server Address (Preferred SIP server)**: enter the primary server IP address number or its URL.
- **Server Address (Alternate SIP server)**: enter the backup SIP server IP address or its URL.
- **SIP Server Port**: set up a SIP server port for data transmission.
- **Registration Period**: set up SIP account registration time span. SIP re-registration will start automatically if the account registration fails during the registration time span. The default registration period is **1800**, ranging from **30-65535s.**

Configure SIP Ports for SIP Calls

You are required to set up a SIP port range for making SIP calls. Navigate to **Account > Advanced > Call.**



Call

Max Local SIP Port	30286	(1024~65535)
Min Local SIP Port	30276	(1024~65535)

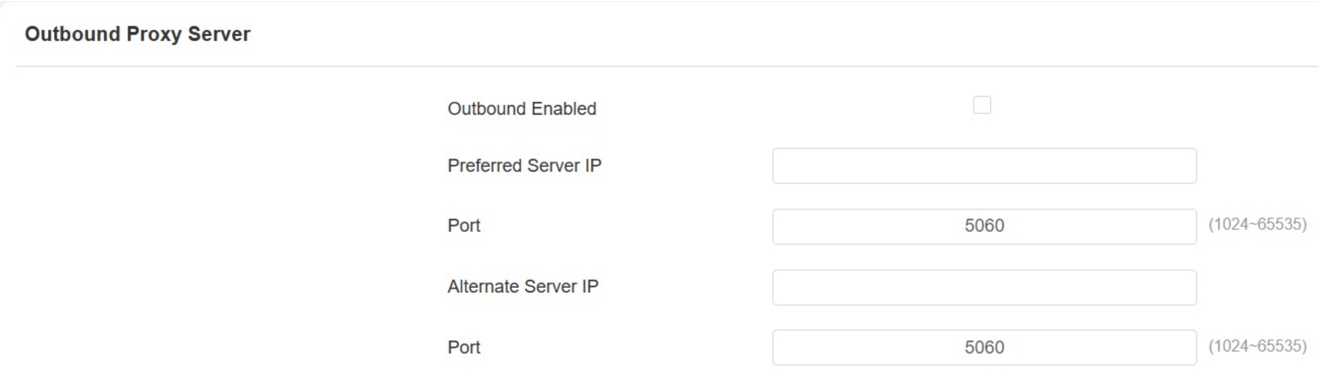
Parameter Set-up:

- **Max Local SIP Port**: enter the maximum SIP port ranging from **1024** to **65535.** The default port setting is 5062.
- **Min Local SIP Port**: enter the minimum SIP port ranging from **1024** to **65535.** The default port setting is 5062.

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.

Path: **Account** > **Basic** > **Outbound Proxy Server**.



Outbound Proxy Server

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

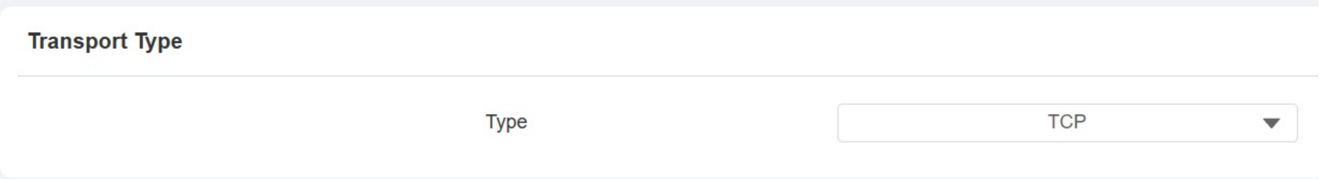
Parameter Set-up:

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

Configure Data Transmission Type

Akuvox intercom devices support four data transmission protocols: **User Datagram Protocol(UDP)**, **Transmission Control Protocol(TCP)**, **Transport Layer Security(TLS)**, and **DNS-SRV**.

Path: **Account** > **Basic** > **Transport Type**.



Transport Type

Type: TCP ▼

Parameter Set-up:

- **UDP**: select **UDP** for 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.
- **DNS-SRV**: select **DNS-SRV** to obtain a DNS record for specifying the location of services. And SRV not only records the server address but also the server port. Moreover, SRV can also be used to configure the priority and the weight of the server address.

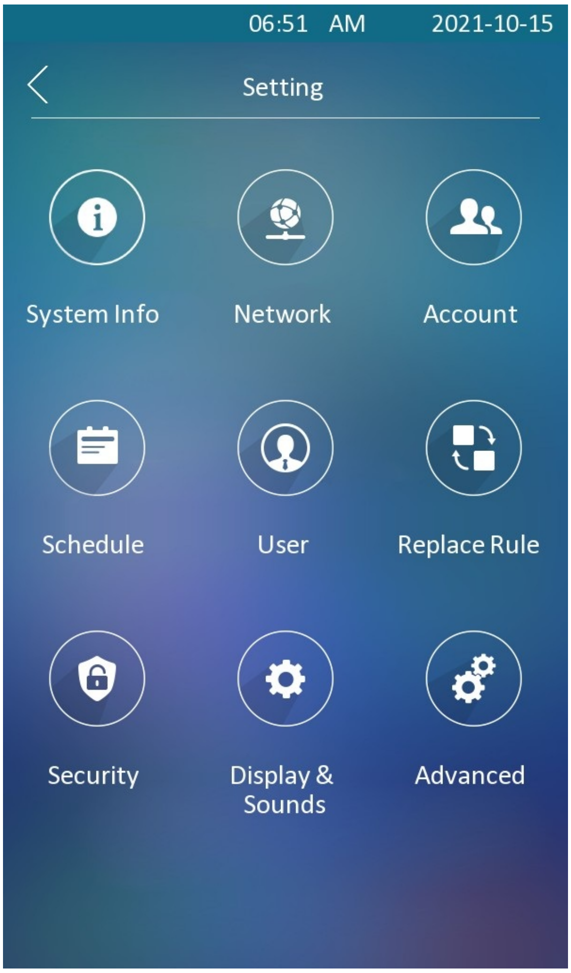
Dial Options Configuration

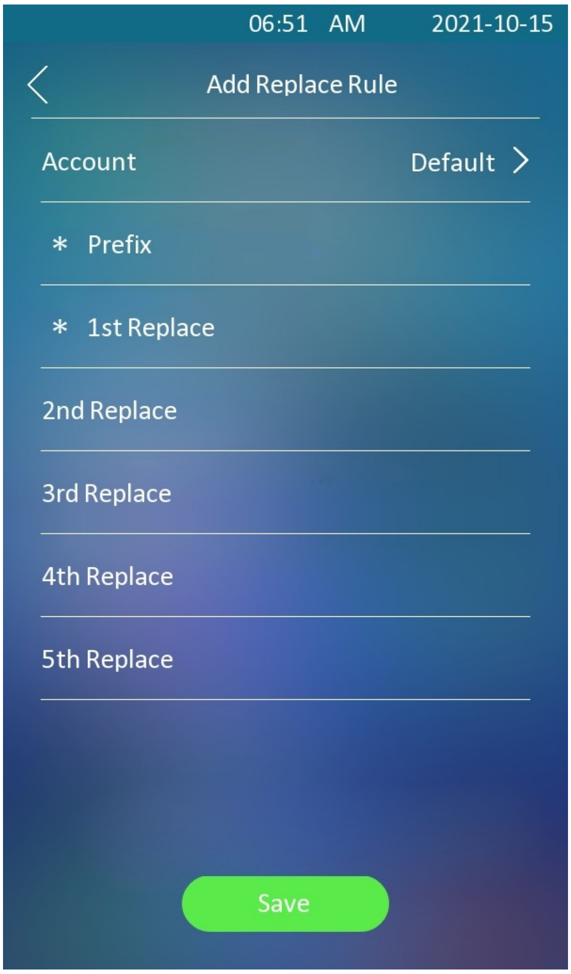
Quick Dial by Number Replacement

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

You can replace the long SIP/IP number with the short number on the device. Path: **Replace Rule > Add Replace Rule.**





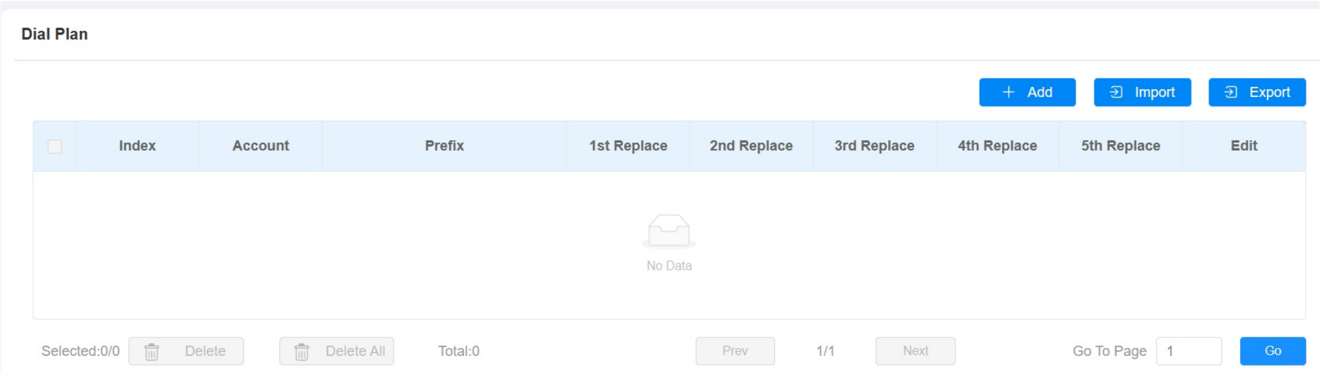
Parameter Set-up:

- **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 dialed 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 dialed number you wish to replace.
- **Replace 1/2/3/4/5**: enter the dialed number(s) you wish to replace. It supports up to 5 number maximum for the replacement on the device configuration. For example, if you replace five original dial numbers with a common short number such as **101** then the five intercom devices with the dialed number will be called at the same time when you dial **101**.

Quick Dial by Number Replacement on the Web

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.

Path: **Intercom > Dial Plan.**



Dial Plan

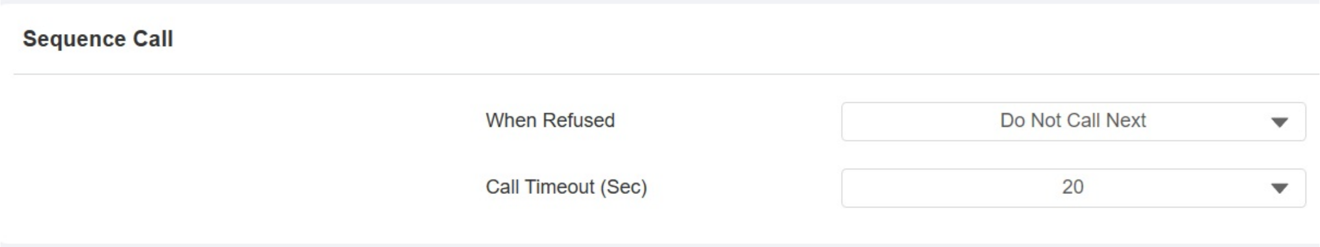
□	Index	Account	Prefix	1st Replace	2nd Replace	3rd Replace	4th Replace	5th Replace	Edit

No Data

Sequence Call

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 do the configuration on the web **Intercom > Basic > Sequence Call** interface.



Sequence Call

When Refused: Do Not Call Next

Call Timeout (Sec): 20

Parameter Set-up:

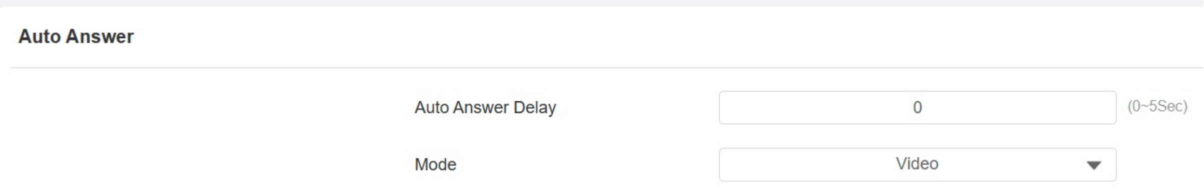
- **When Refused**: if you select **Do Not Call Next**, then the sequence call will be terminated if the call is rejected by the called party. If you select **Call Next** then the sequence call will be continued to the next called party if it is rejected by the first called party.

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.

- Configure auto-answer function

  Path: **Intercom > Call Feature > Auto Answer**.



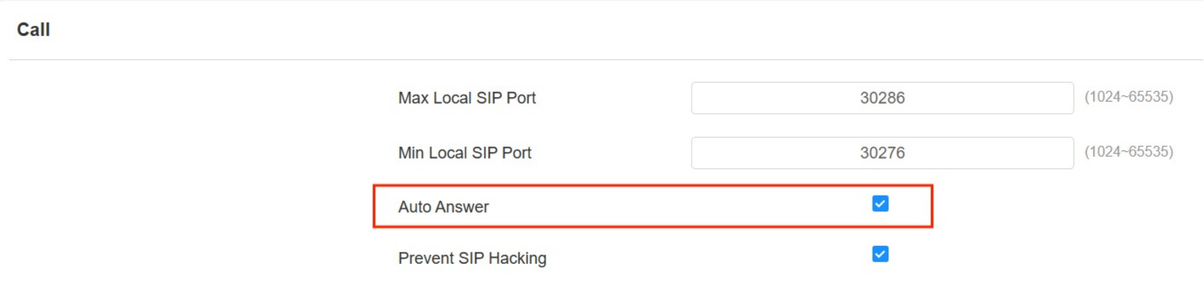
Auto Answer

Auto Answer Delay: 0 (0~5Sec)

Mode: Video

- Enable Auto-answer mode

  Path: **Account > Advanced > Call.**



Call

Max Local SIP Port: 30286 (1024~65535)

Min Local SIP Port: 30276 (1024~65535)

Auto Answer ☑

Prevent SIP Hacking ☑

Parameter Set-up:

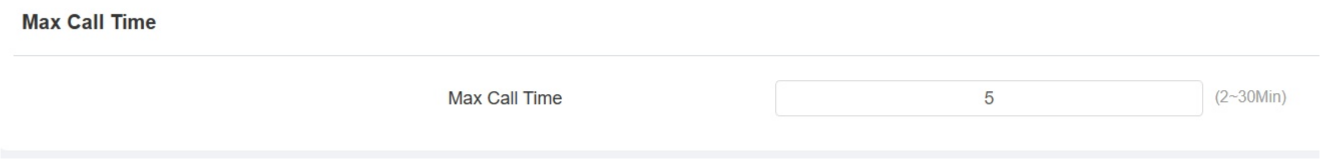
- **Auto Answer Delay**: set up the delay time (**from 0-5 sec.**) before the call can be answered automatically. For example, if you set the delay time as 1 second, then the call will be answered in 1 second automatically.
- **Auto Answer Mode**: set up the **Video** or **Audio** mode you preferred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

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.

Path: **Intercom > Call Feature > Max Call Time**



Max Call Time

Max Call Time: 5 (2~30Min)

Parameter Set-up:

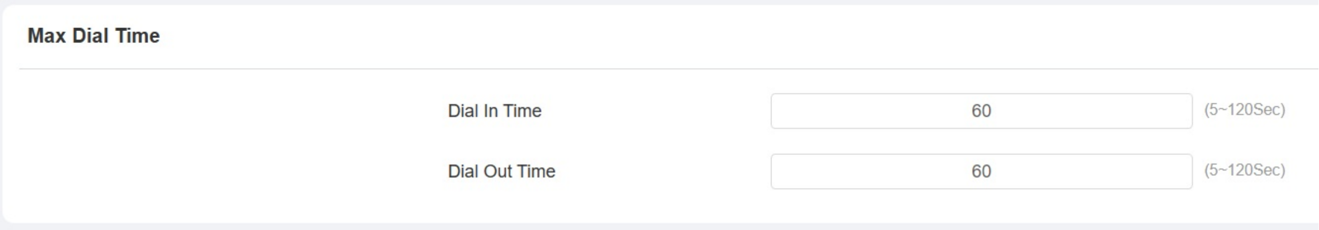
- **Max Call Time**: enter the call time duration according to your need (ranging from 2-30 min.). The default call time duration is 5 min.

> **Note**
>
> - The max call time of the device is also related to the max call time of the SIP server. If using a SIP account to make a call, please pay attention to the max call time of the SIP server. If the max call time of the SIP server is shorter than the max call time of the device, the shorter one is available.

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.

Path: **Intercom > Call Feature> Max Dial Time**.



Max Dial Time

Dial In Time: 60 (5~120Sec)

Dial Out Time: 60 (5~120Sec)

Parameter Set-up:

- **Dial In Time**: enter the dial-in time duration for your door phone (**ranging from 30-120 sec.**). 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 5-120 sec.**). 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 to.

Note

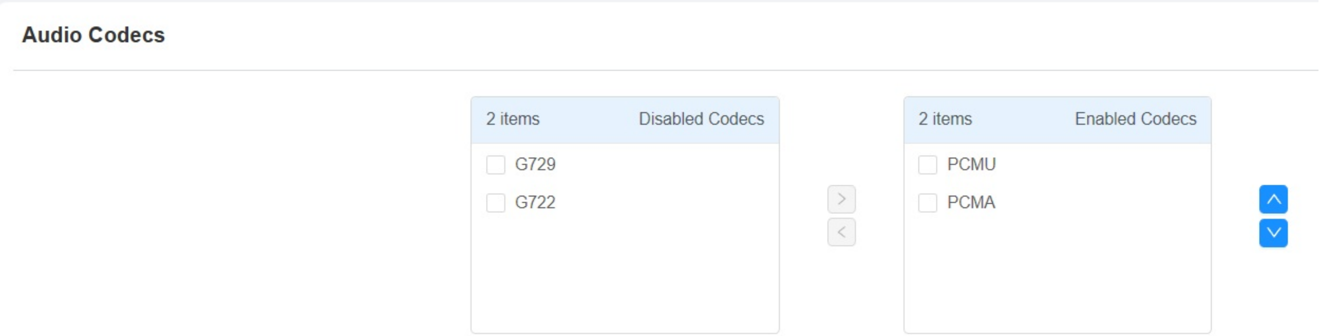
- Max dial time of the device is also related to the max dial time of the SIP server. If using an SIP account to make a call, please pay attention to the max dial time of the SIP server. If the max dial time of the SIP server is shorter than the max dial time of the device, the shorter one is available.

Audio& Video Codec Configuration for SIP Calls

Configure Audio Codec

The door phone supports four types of Codec (PCMU, PCMA, G729, 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.

Path: **Account > Advanced > Audio Codecs.**

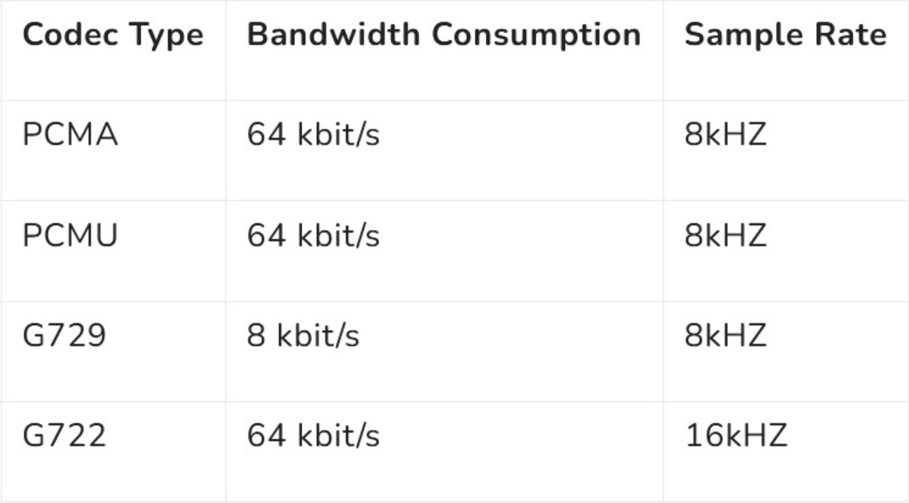


Audio Codecs

2 items	Disabled Codecs
□ G729	
□ G722	

2 items	Enabled Codecs
□ PCMU	
□ PCMA	

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

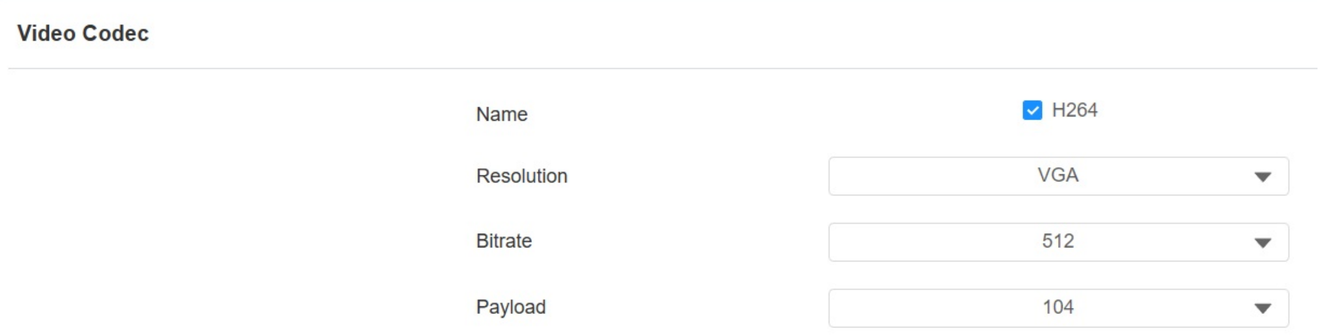


Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G729	8 kbit/s	8kHZ
G722	64 kbit/s	16kHZ

Configure Video Codec

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

Path: **Account > Advanced > Video Codecs.**



Video Codec

Name	☑ H264
Resolution	VGA
Bitrate	512
Payload	104

Parameter Set-up:

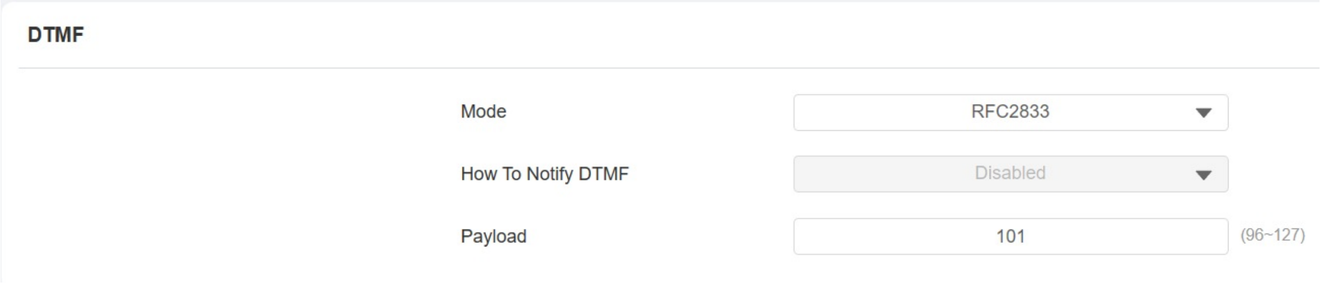
- **Name**: Check to select the H264 video codec format for the door phone video stream. H264 is the video codec by default.
- **Resolution**: select the code resolution for the video quality among five options: **QCIF, CIF, VGA, 4CIF**, and **720P** according to your actual network environment. The default code resolution is **VGA.**
- **Bitrate**: select the video stream bit rate (ranging from **128-2048**). 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.

- **Payload**: select the payload type (ranging from **90-119**) to configure the audio codec payload. The payload between the door phone and the corresponding intercom device should be identical. 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.

Path: **Account** > **Advanced** > **DTMF**.



DTMF

Mode: RFC2833

How To Notify DTMF: Disabled

Payload: 101 (96~127)

Parameter Set-up:

- **Mode**: select DTMF mode among six options: **Inband**, **RFC2833**, **Info**, **Info+Inband**, **Info+RFC2833**, and **Info+Inband+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.

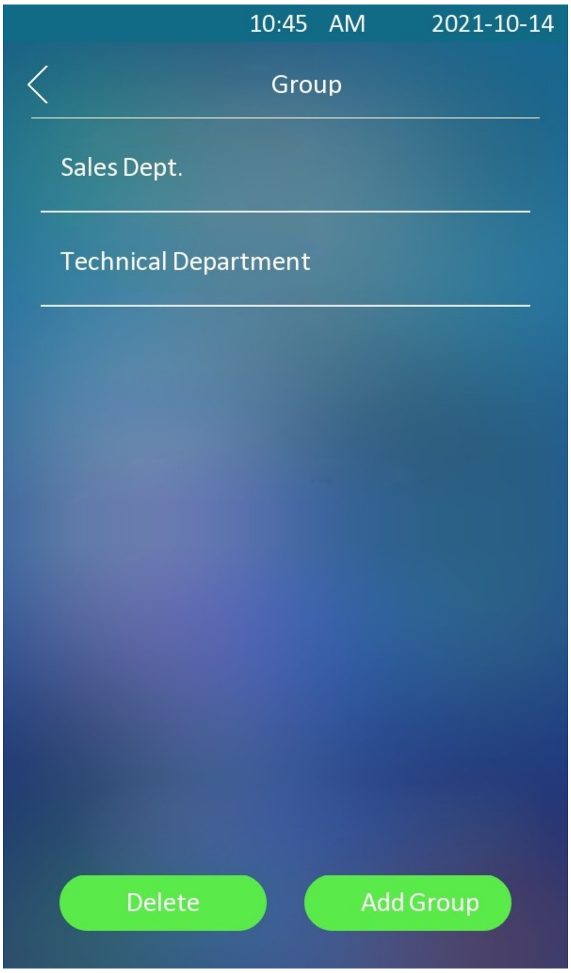
- **Payload**: set the payload according to the specific data transmission payload agreed on between the sender and receiver during the data transmission.

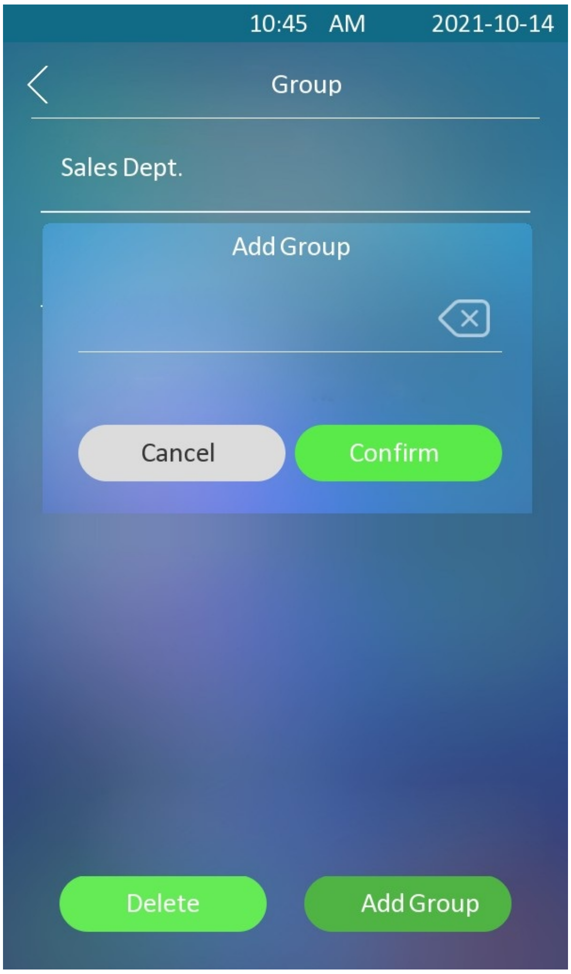
Phone Book Configuration

Phone Book Configuration on the Device

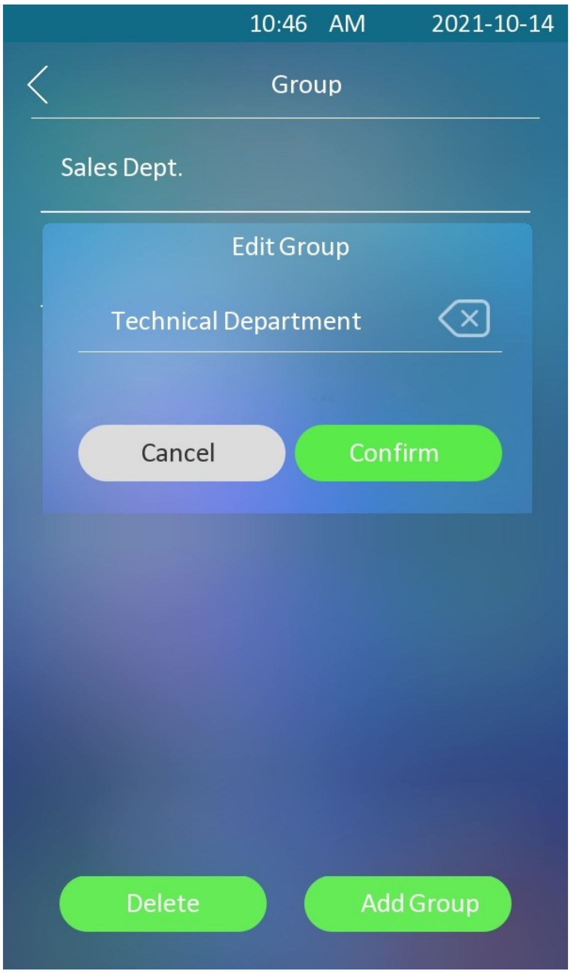
You can create contact groups for users.

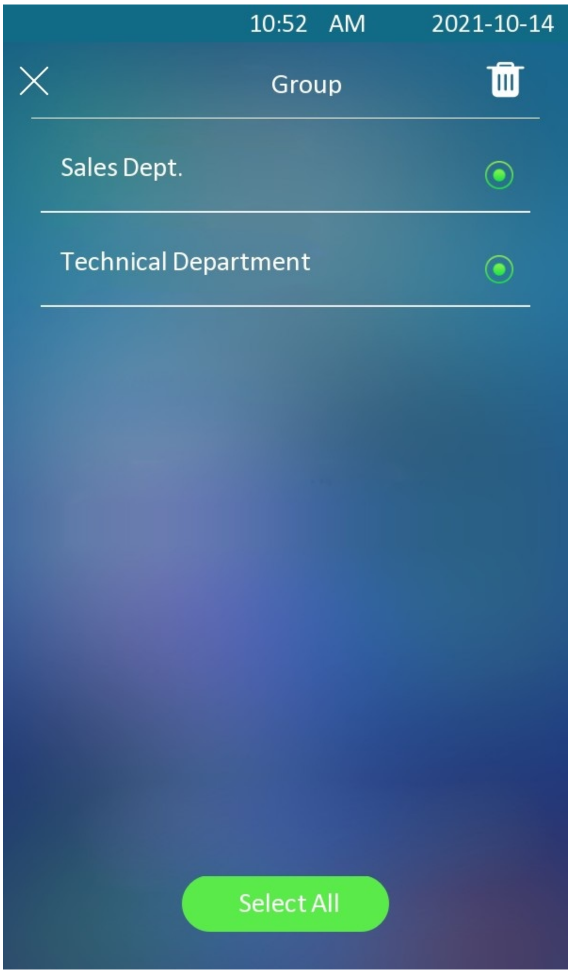
To configure the phone book on the device **User > Group**.





10:45 AM
2021-10-14
Group
Sales Dept.
Add Group
Cancel
Confirm
Delete
Add Group


10:46 AM
2021-10-14
Group
Sales Dept.
Edit Group
Technical Department
Cancel
Confirm
Delete
Add Group



10:52 AM 2021-10-14

Group

Sales Dept. ●

Technical Department ●

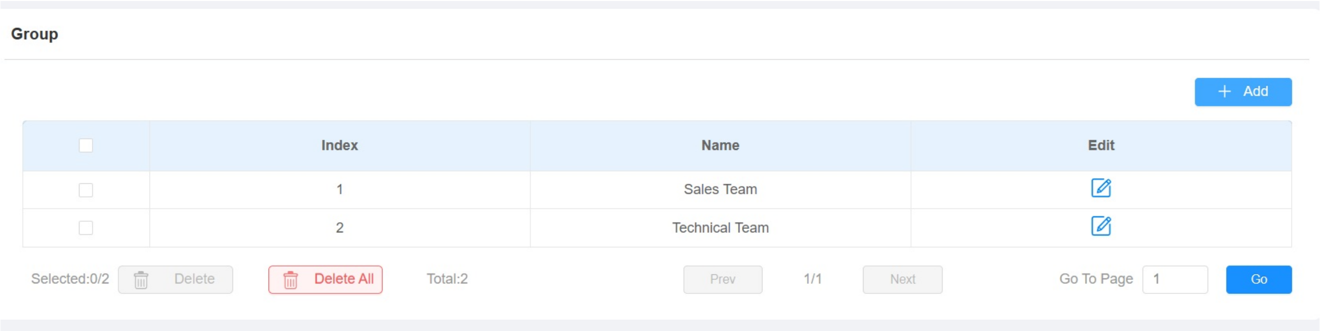
Select All

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.

Path: **Directory > User> Group.**



Group

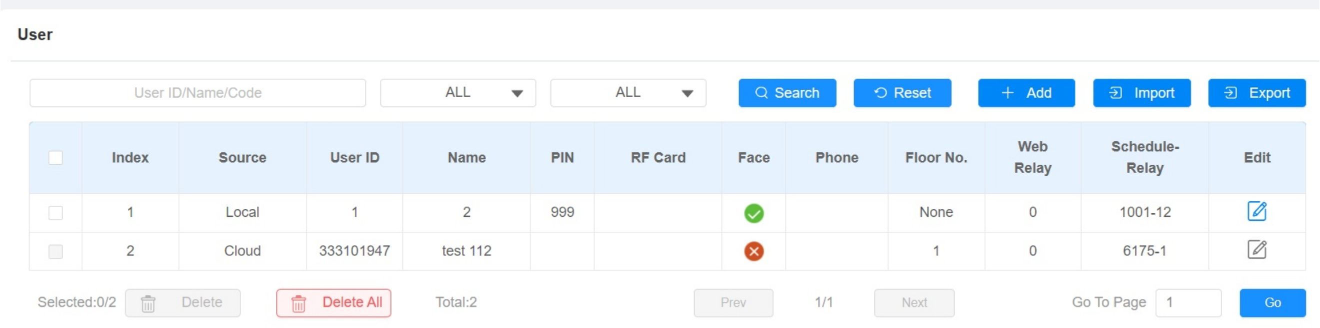
+ Add

□	Index	Name	Edit
□	1	Sales Team	✎
□	2	Technical Team	✎

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

Contact List Configuration on the Web Interface

Contact can also be configured on the web interface where you can also upload the contact pictures if needed. To configure the configuration on the web **Directory > User** interface.



User

User ID/Name/Code | ALL ▾ | ALL ▾ | Search | Reset | + Add | Import | Export

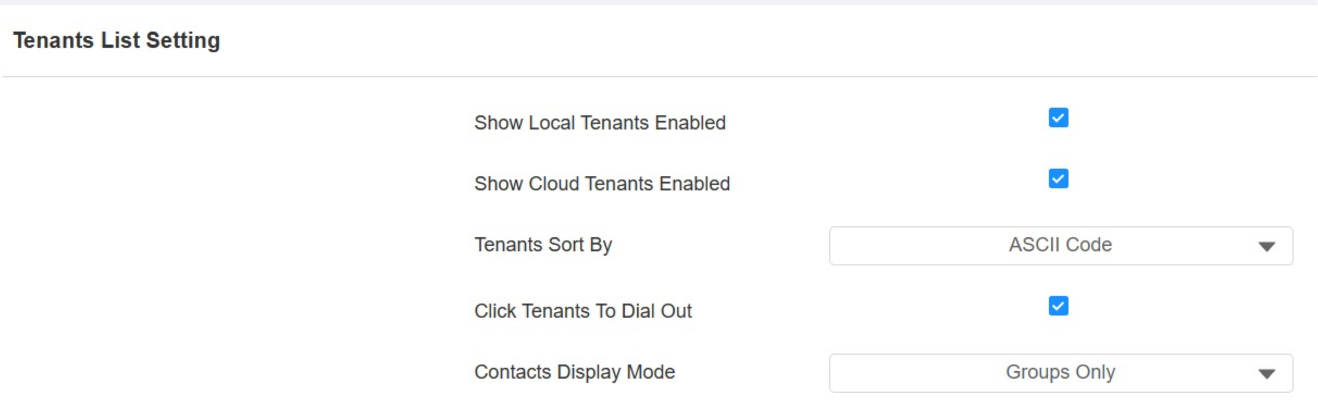
□	Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
□	1	Local	1	2	999		✓		None	0	1001-12	✎
□	2	Cloud	333101947	test 112			✗		1	0	6175-1	✎

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

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.

Path: **Directory > Directory Setting> Tenants List Setting**.



Tenants List Setting

Show Local Tenants Enabled	☑
Show Cloud Tenants Enabled	☑
Tenants Sort By	ASCII Code ▾
Click Tenants To Dial Out	☑
Contacts Display Mode	Groups Only ▾

Parameter Set-up:

- **Show Local Tenants Enabled**: tick or untick the check box to control the display of the group label. If you untick the check box, then only the group tab will be displayed while the contact tab will be concealed and vice versa.
- **Show Cloud Tenants Enabled**: tick the check box to show the cloud tenants in the tenants list. And when you untick the check box, the cloud tenants will be concealed.
- **Tenants Sort By**: select **ASCII Code, 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. When you select **Import**, the contacts will be sorted in the order in the import file.
- **Click Tenants 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

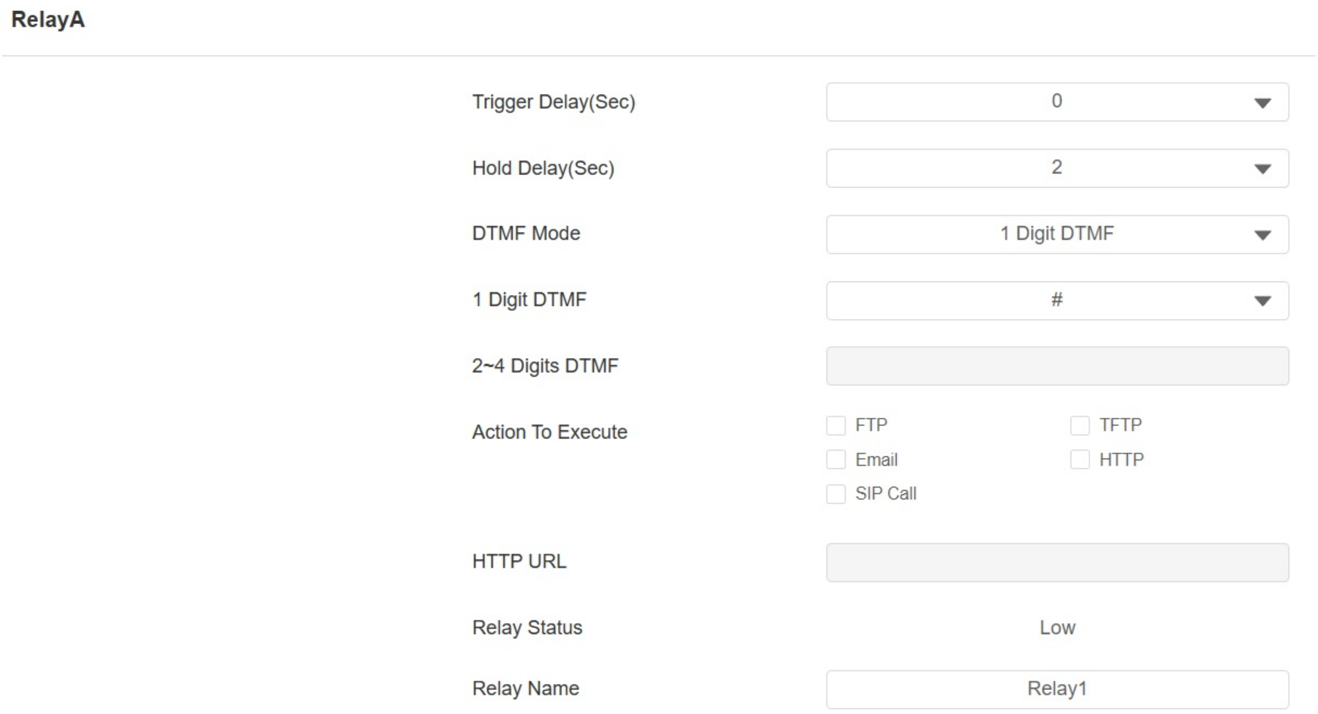
dial out. This function will be disabled when you untick the check box, and when it is disabled, you need to press the Call icon to dial out.

- **Contacts Display Mode**: Select from **Groups Only, All Contacts**, and **Group On Entry Page And Their Contacts On Subpage**. If you select **Groups Only**, you can tap the group to call all contacts. The group name is displayed when calling.

Relay Setting

Relay Switch Setting

You can unlock the door via DTMF code during the call. To do so, you are required to set up DTMF code along with relays. Path: **Access Control > Relay > RelayA**



RelayA

Trigger Delay(Sec)	0
Hold Delay(Sec)	2
DTMF Mode	1 Digit DTMF
1 Digit DTMF	#
2~4 Digits DTMF	
Action To Execute	□ FTP □ TFTP □ Email □ HTTP □ SIP Call
HTTP URL	
Relay Status	Low
Relay Name	Relay1

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 after the door is unlocked.
- **DTMF Mode**: select the number of DTMF digit for the door access control (ranging from 1-4 digit) For example, you can select 1-digit DTMF code or 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** setting. For example, you are required to set the 3-digit DTMF code if **DTMP Mode** is set as 3- digit.
- **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.

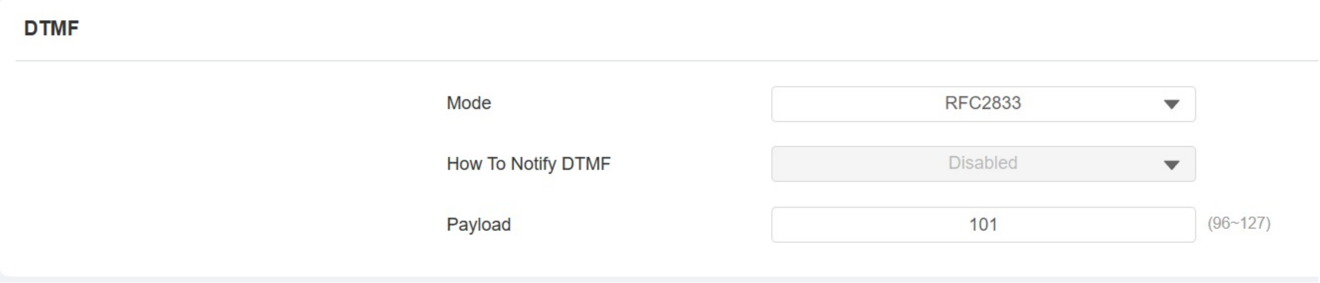
Note

- 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 DTMF code in **2~4 Digits DTMF** field. And if you set DTMF mode from 2-4 in **2~4 Digits DTMF** field, you cannot edit DTMF code in **1 Digit DTMF** field.

DTMF Code Configuration

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.

Path: **Account > Advanced > DTMF.**



DTMF

Mode: RFC2833

How To Notify DTMF: Disabled

Payload: 101 (96~127)

Parameter Set-up:

- **Mode**: select DTMF type among six options: **Inband, RFC2833, Info, Info+Inband, Info+RFC2833**, and **Info+Inband+RFC2833** according to your need.
- **DTMF Code Transport format**: select among four options: **Disable, DTMF, DTMF-Relay, Telephone-Event** according to your need.
- **Payload**: select payload 96-127 for data transmission identification. The default payload is 101.

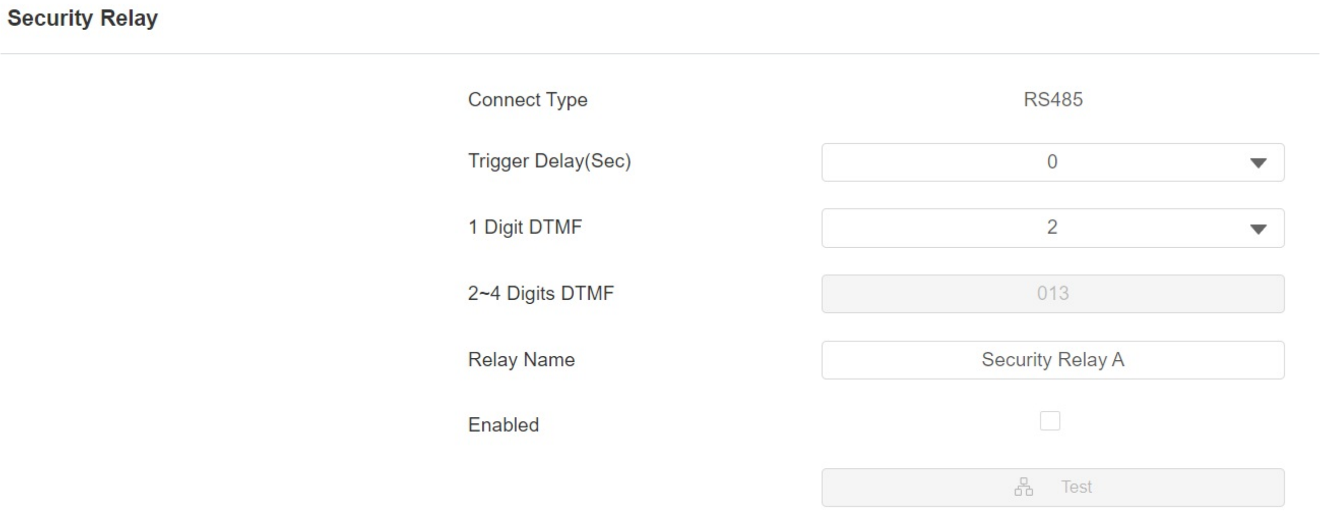
Note

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

Security Relay Setting

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**.



Security Relay

Connect Type	RS485
Trigger Delay(Sec)	0
1 Digit DTMF	2
2~4 Digits DTMF	013
Relay Name	Security Relay A
Enabled	□
	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.
- **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.

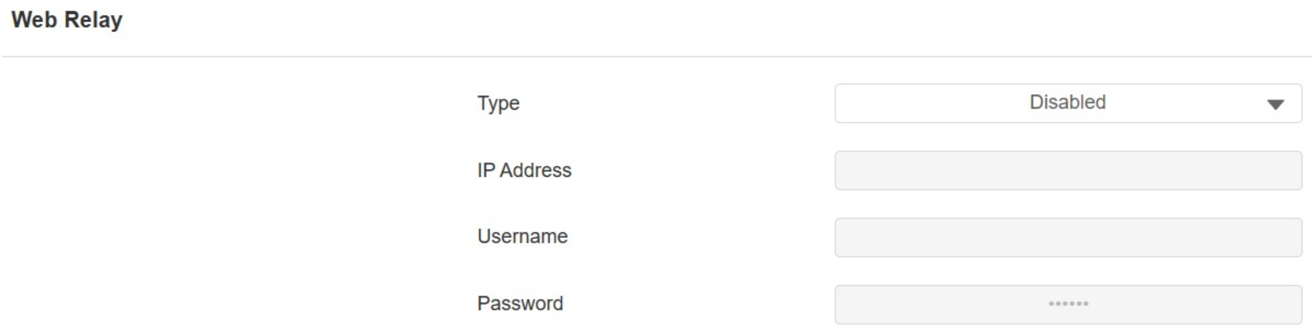
Web Relay Setting

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.

Path: **Access Control > Web Relay.** IP Address, User Name, and Password are provided by the web relay manufacturer.



Web Relay

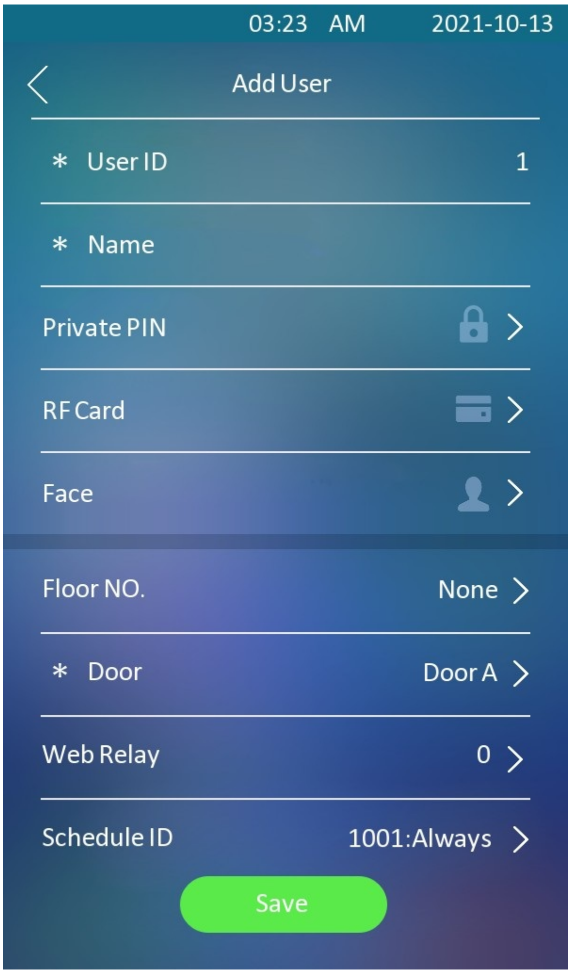
Type	Disabled
IP Address	
Username	
Password	••••••

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 passwords are 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 DTMF code, the action command will be sent to the web relay automatically.
- **Web Relay Extension**: enter the relay extension information, which can be a SIP Account user name of an intercom device such as an indoor monitor, so that the specific action command will be sent when unlock is performed on the intercom device, while this setting is optional. And please refer to the example below: **http://admin:admin@192.168.1.2/state.xml?relayState=2**.

Configure Web Relay on the Device

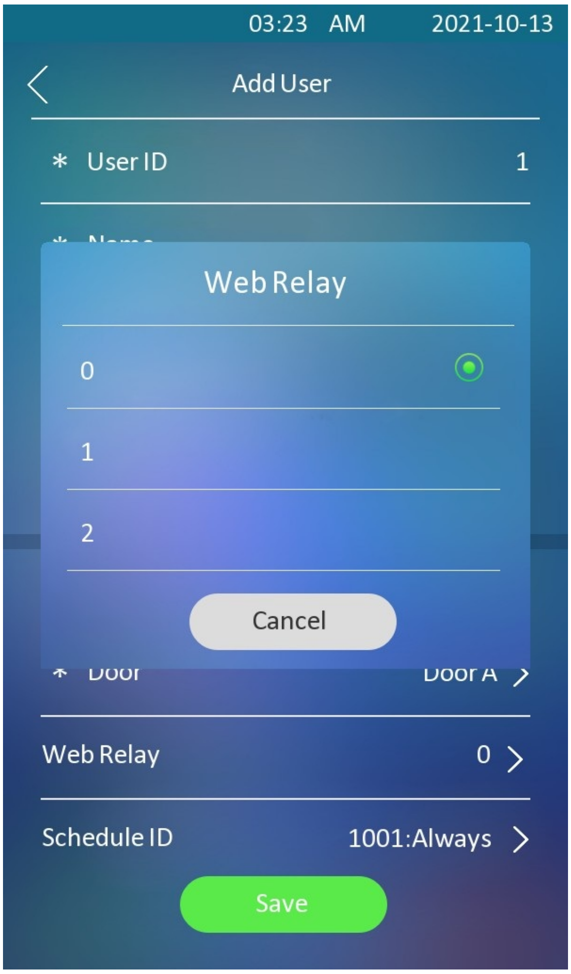
After the web relay actions are entered on the web interface, you can now select the specific number of the web relay actions to be carried for the specific resident you added for the door unlock. Path: **User > User List.**



03:23 AM 2021-10-13

Add User

* User ID	1
* Name	
Private PIN	>
RF Card	>
Face	>
Floor NO.	None >
* Door	Door A >
Web Relay	0 >
Schedule ID	1001:Always >



03:23 AM 2021-10-13

Add User

* User ID 1

* Name

Web Relay

0 ●

1

2

Cancel

* Door Door A

Web Relay 0

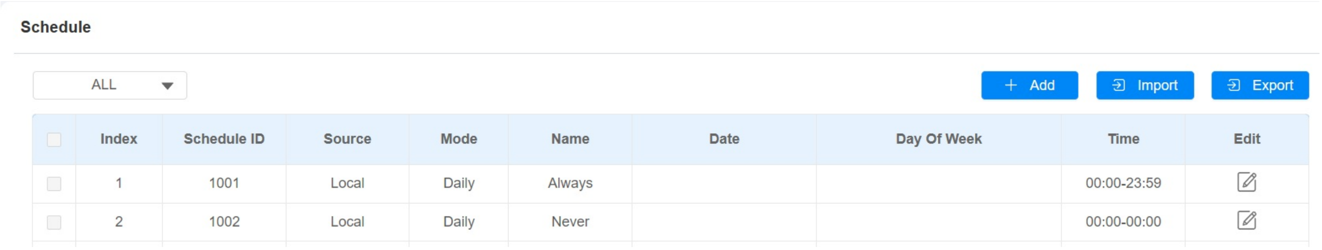
Schedule ID 1001:Always

Save

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.

You are required to set the relay schedule first before applying the relay schedule to the specific relay for the door access control. Path: **Setting > Schedule**.

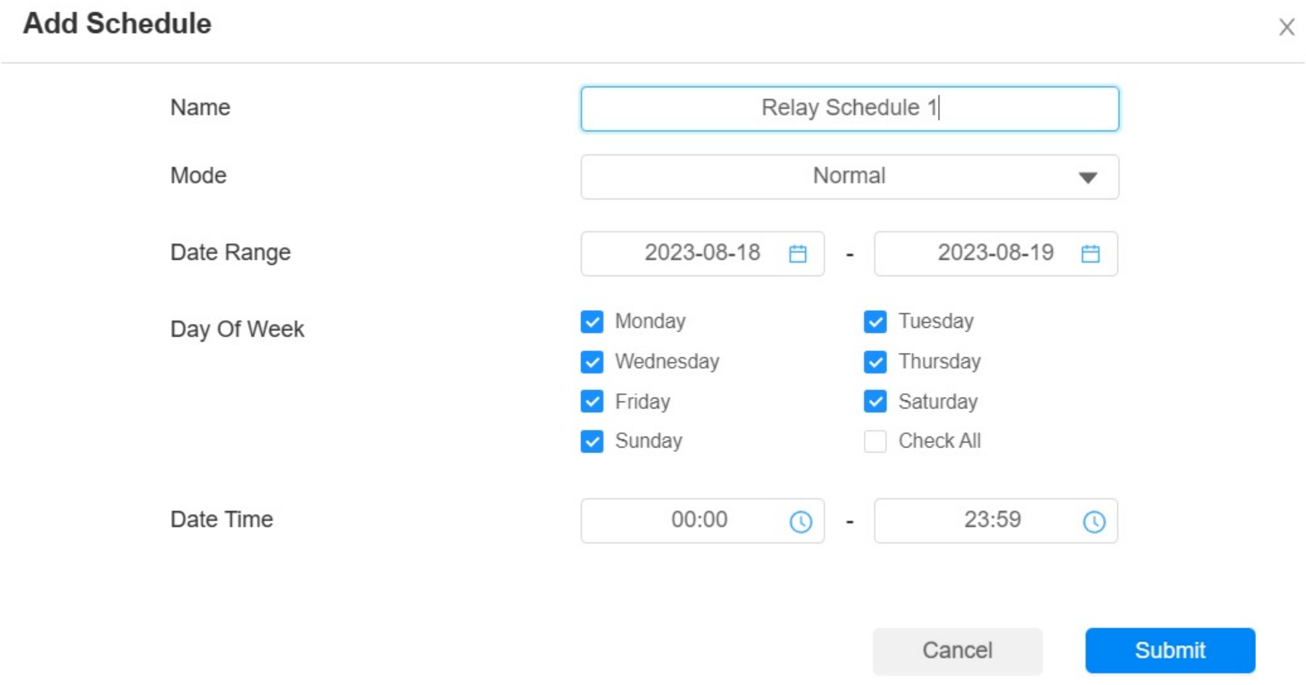


Schedule

ALL ▾

＋ Add Import Export

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



Add Schedule

Name: Relay Schedule 1

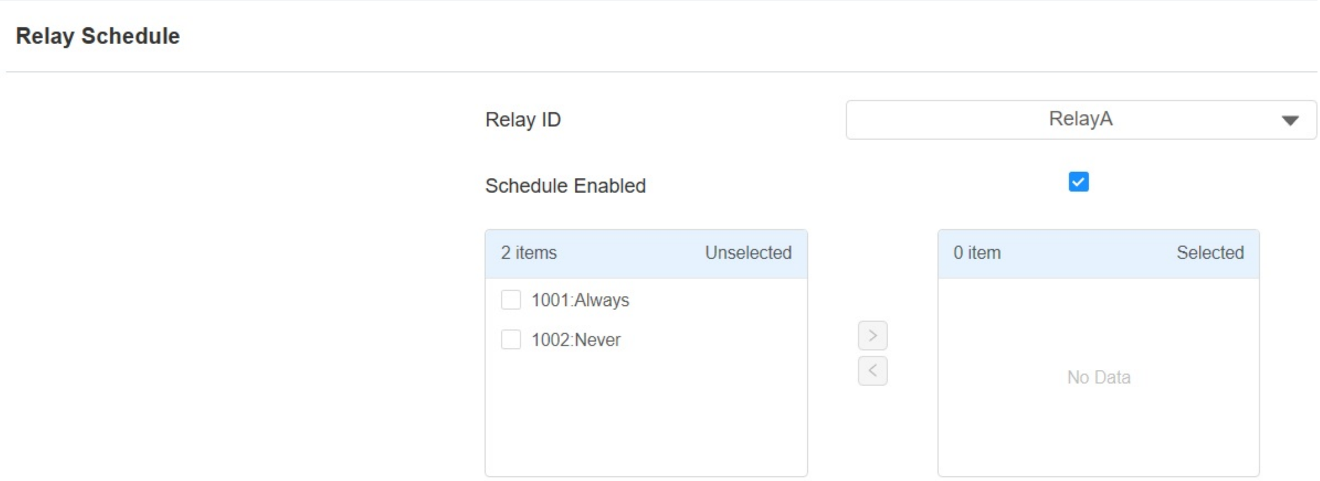
Mode: Normal

Date Range: 2023-08-18 - 2023-08-19

Day Of Week: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday □ Check All

Date Time: 00:00 - 23:59

After the relay schedule is created, you can select the relay schedule and select the specific relay to which you want to apply the schedule. Path: **Access control > Relay > Relay Schedule.**



Relay Schedule

Relay ID: RelayA

Schedule Enabled: ☑

2 items Unselected
□ 1001:Always
□ 1002:Never

0 item Selected
No Data

Note

- You can refer to **Create Door Access Schedule** for the relay schedule setting.

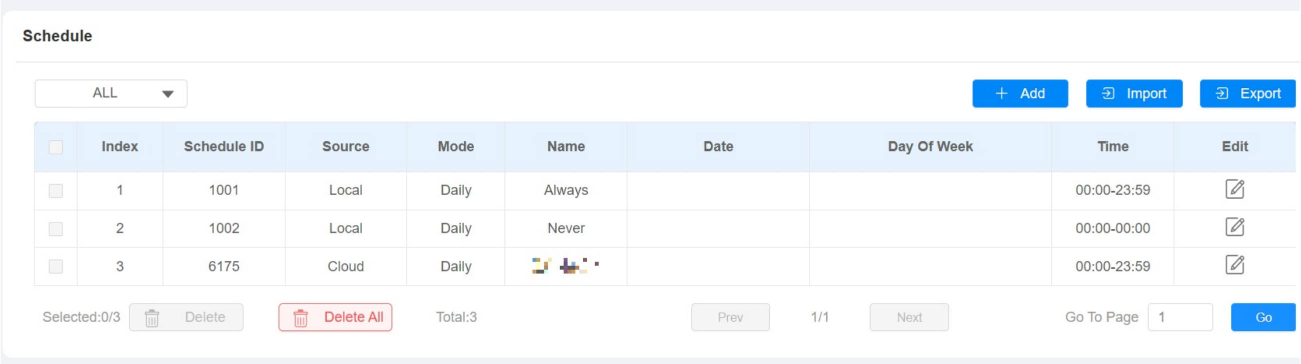
Door Access Schedule Management

Configure Door Access Schedule

A door access schedule lets you decide who can open the door and when. It applies to both individuals and groups, ensuring that users within the schedule can only open the door using the authorized method during designated time periods.

Create Door Access Schedule on the Web Interface

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 the schedule, go to **Setting > Schedule**, then click + Add .



Schedule

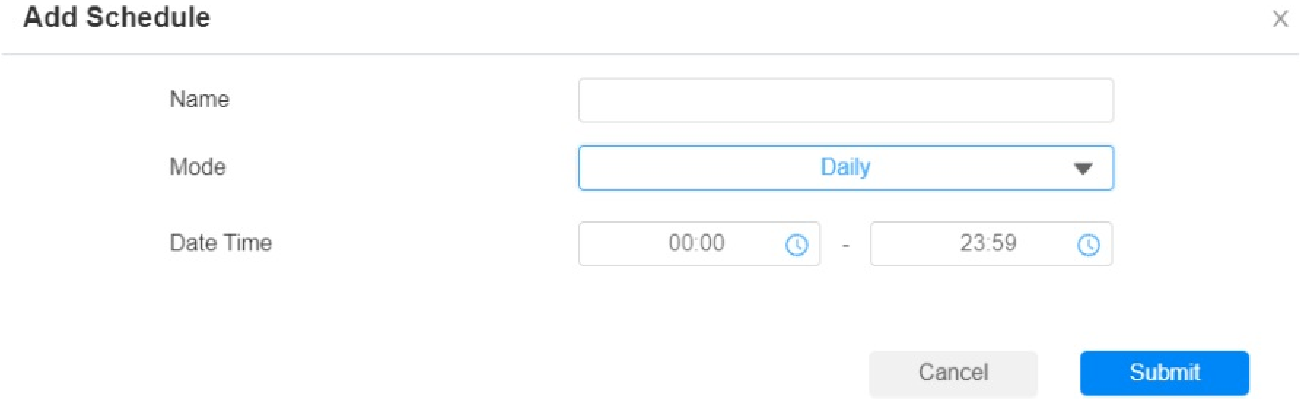
ALL ▾

+ Add | Import | Export

□	Index	Schedule ID	Source	Mode	Name	Date	Day Of Week	Time	Edit
□	1	1001	Local	Daily	Always			00:00-23:59	✎
□	2	1002	Local	Daily	Never			00:00-00:00	✎
□	3	6175	Cloud	Daily	[redacted]			00:00-23:59	✎

Selected:0/3 Delete Delete All Total:3 Prev 1/1 Next Go To Page 1 Go

To create a daily schedule:

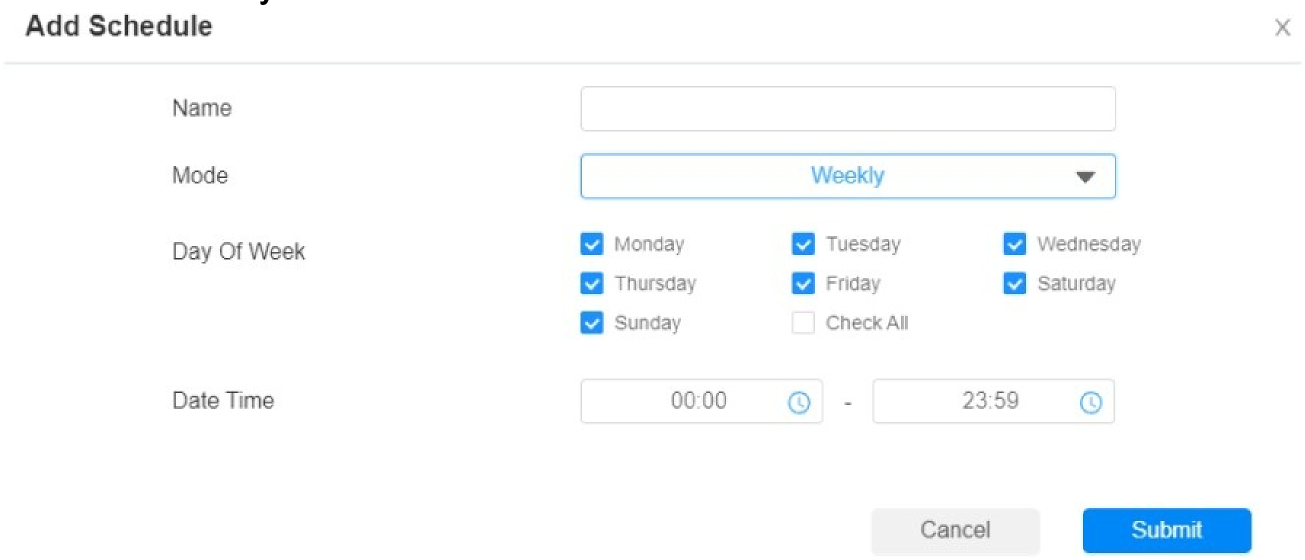


Add Schedule ×

Name	
Mode	Daily ▾
Date Time	00:00 - 23:59

Cancel Submit

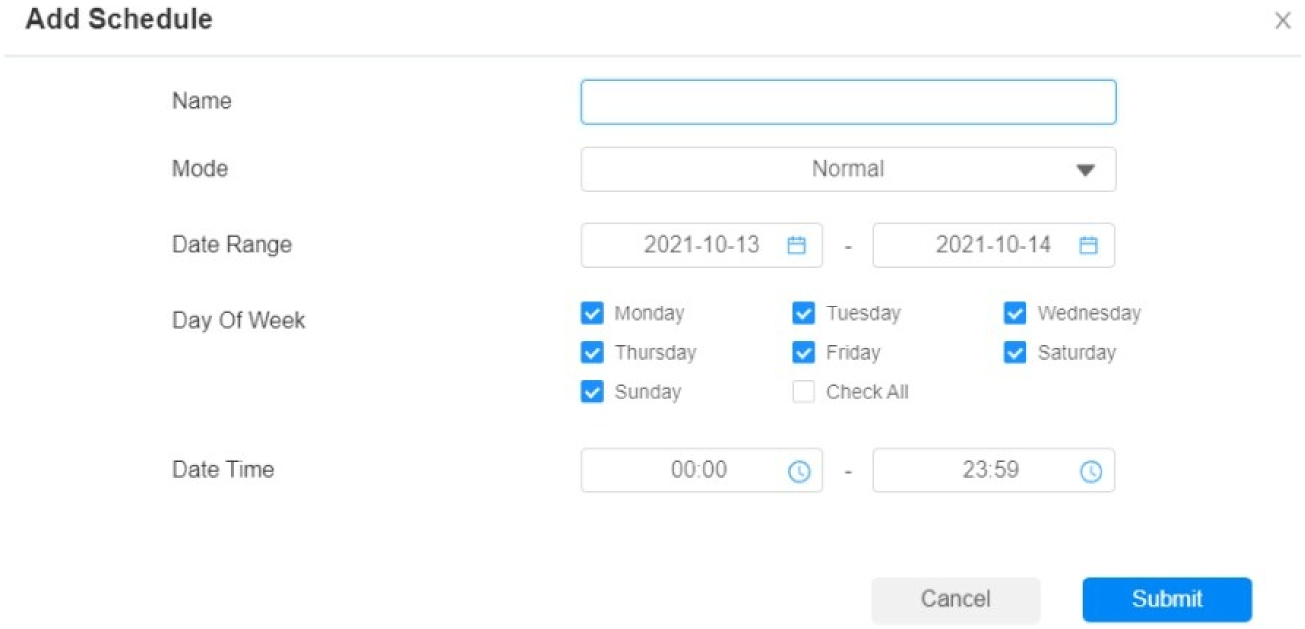
To create a weekly schedule:



Add Schedule

Name	
Mode	Weekly ▾
Day Of Week	☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday □ Check All
Date Time	00:00 - 23:59

To create a longer period schedule:

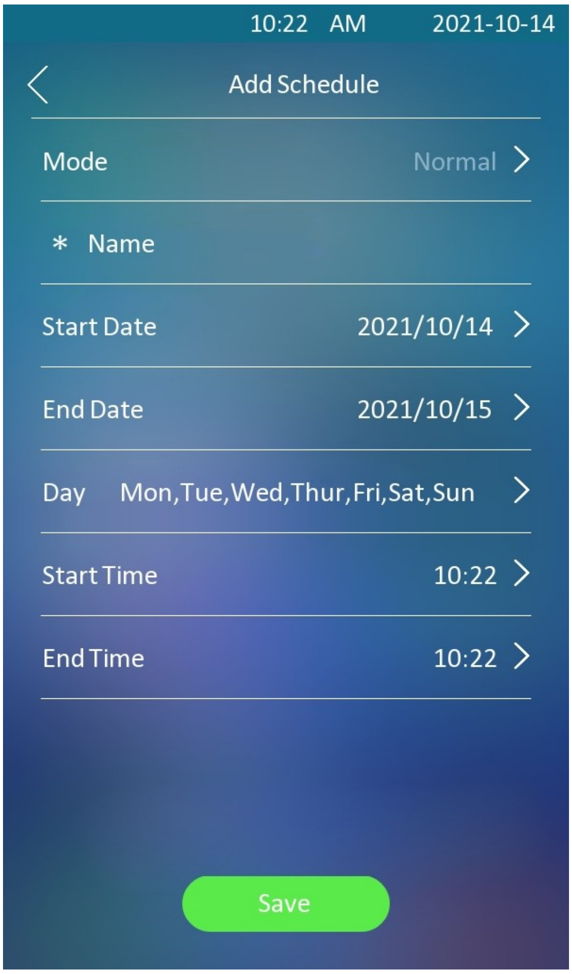


Add Schedule

Name	
Mode	Normal ▾
Date Range	2021-10-13 - 2021-10-14
Day Of Week	☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday □ Check All
Date Time	00:00 - 23:59

Create Door Access Schedule on the Device

You can also create a door access schedule on the device. Path: **Schedule > Add Schedule**.



10:22 AM 2021-10-14

Add Schedule

Mode: Normal

* Name

Start Date: 2021/10/14

End Date: 2021/10/15

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

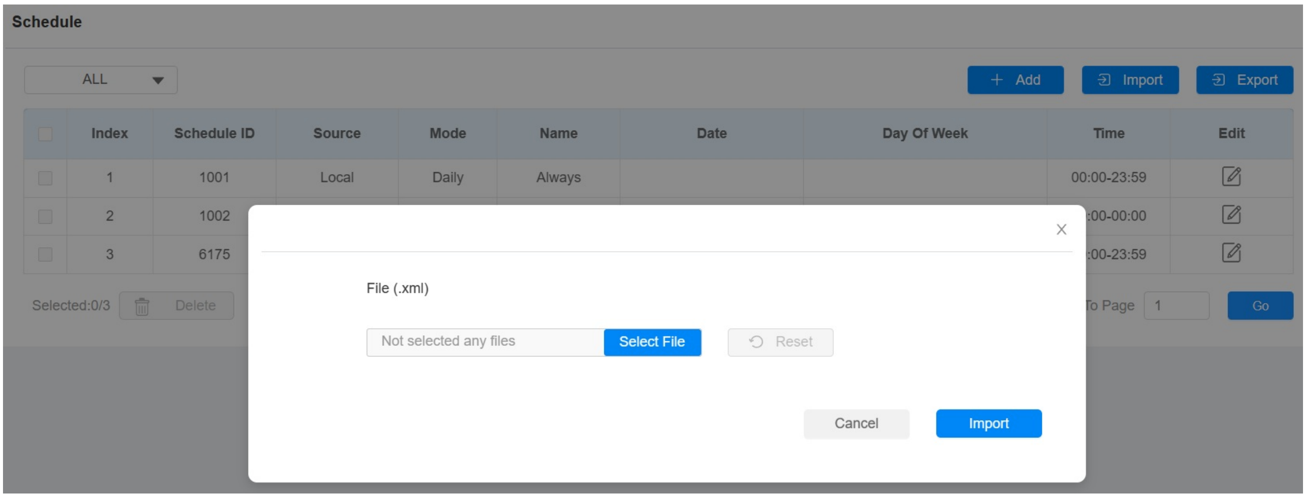
Start Time: 10:22

End Time: 10:22

Import and Export Door 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.

Path: **Setting > Schedule**.



Schedule

□	Index	Schedule ID	Source	Mode	Name	Date	Day Of Week	Time	Edit
□	1	1001	Local	Daily	Always			00:00-23:59	
□	2	1002						:00-00:00	
□	3	6175						:00-23:59	

Selected:0/3

File (.xml)

Not selected any files

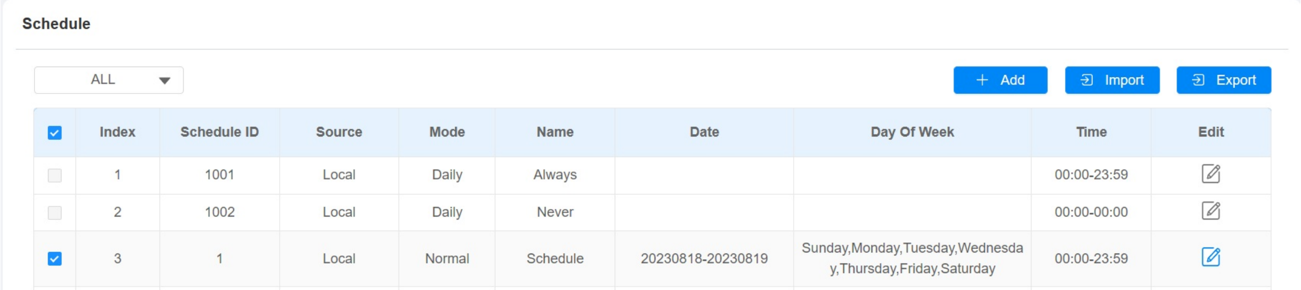
Note

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

Edit the Door Access Schedule

Edit the Door Access Schedule on the Web Interface

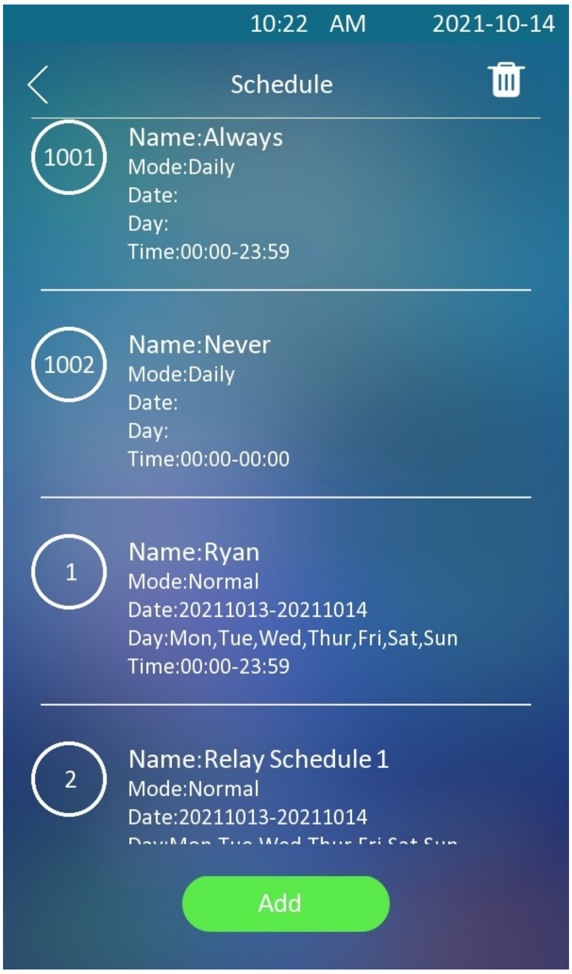
If you want to edit or delete the door access schedule you created, you can edit or delete the configured schedule separately or in batch on the web interface. Path: **Setting > Schedule**.



Schedule

☑	Index	Schedule ID	Source	Mode	Name	Date	Day Of Week	Time	Edit
□	1	1001	Local	Daily	Always			00:00-23:59	✎
□	2	1002	Local	Daily	Never			00:00-00:00	✎
☑	3	1	Local	Normal	Schedule	20230818-20230819	Sunday,Monday,Tuesday,Wednesday,Thursday,Friday,Saturday	00:00-23:59	✎

You can also edit or delete the door access schedule on the device. Path: **Schedule > Schedule**.



10:22 AM 2021-10-14

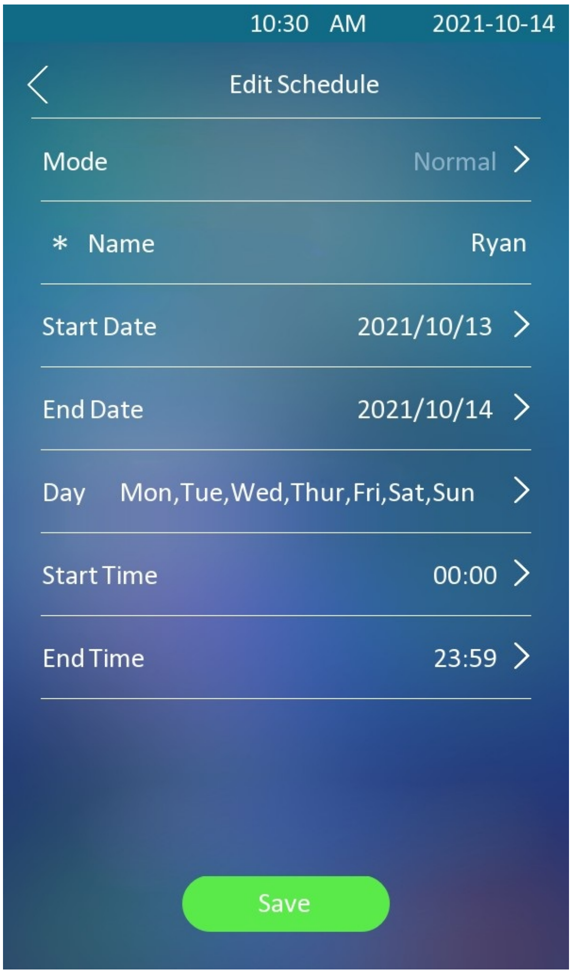
Schedule

1001
Name:Always
Mode:Daily
Date:
Day:
Time:00:00-23:59

1002
Name:Never
Mode:Daily
Date:
Day:
Time:00:00-00:00

1
Name:Ryan
Mode:Normal
Date:20211013-20211014
Day:Mon,Tue,Wed,Thur,Fri,Sat,Sun
Time:00:00-23:59

2
Name:Relay Schedule 1
Mode:Normal
Date:20211013-20211014
Day:Mon,Tue,Wed,Thur,Fri,Sat,Sun



10:30 AM 2021-10-14

Edit Schedule

Mode Normal

* Name Ryan

Start Date 2021/10/13

End Date 2021/10/14

Day Mon,Tue,Wed,Thur,Fri,Sat,Sun

Start Time 00:00

End Time 23:59

Door Unlock Configuration

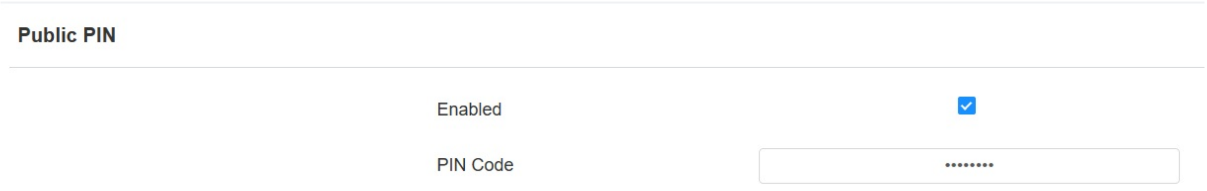
Configure PIN Code for Door Unlock

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 and modify public PIN codes on the device and on the device's web interface.

- **Configure public PIN code on the web interface**
  Path: **Access Control > PIN Setting > Public PIN**



Public PIN

Enabled ☑

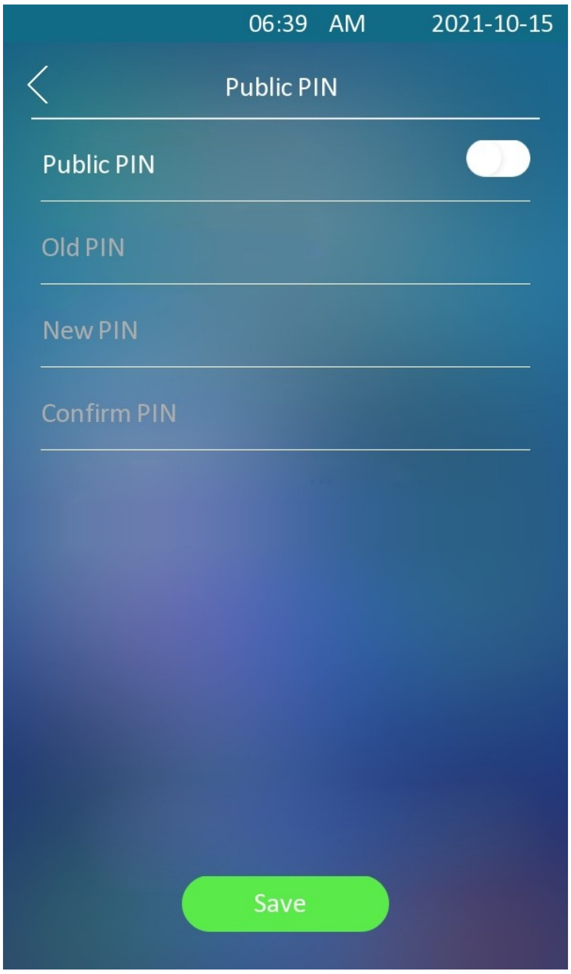
PIN Code ••••••••

Parameter Set-up:

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

- **Configure the public PIN code on the device**

Path: **Security > Public PIN.**



Public PIN

Old PIN

New PIN

Confirm PIN

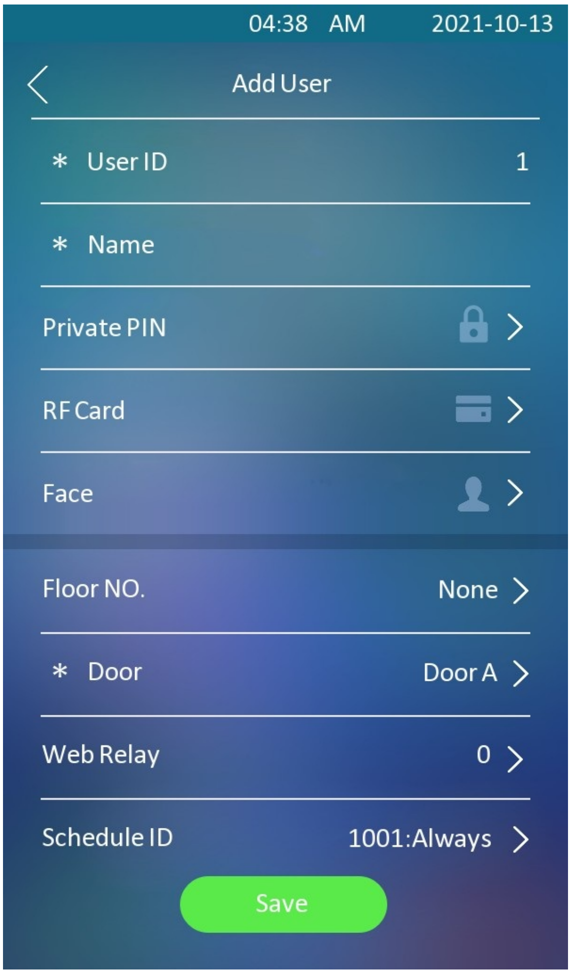
Note

- The public PIN code will not be valid until the function is turned on.
- **APT+PIN** can only be applicable when the device is added to the Akuvox SmartPlus.

Configure Private PIN Code on the Device

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

Path: **User > User List**



04:38 AM 2021-10-13

Add User

* User ID 1

* Name

Private PIN

RF Card

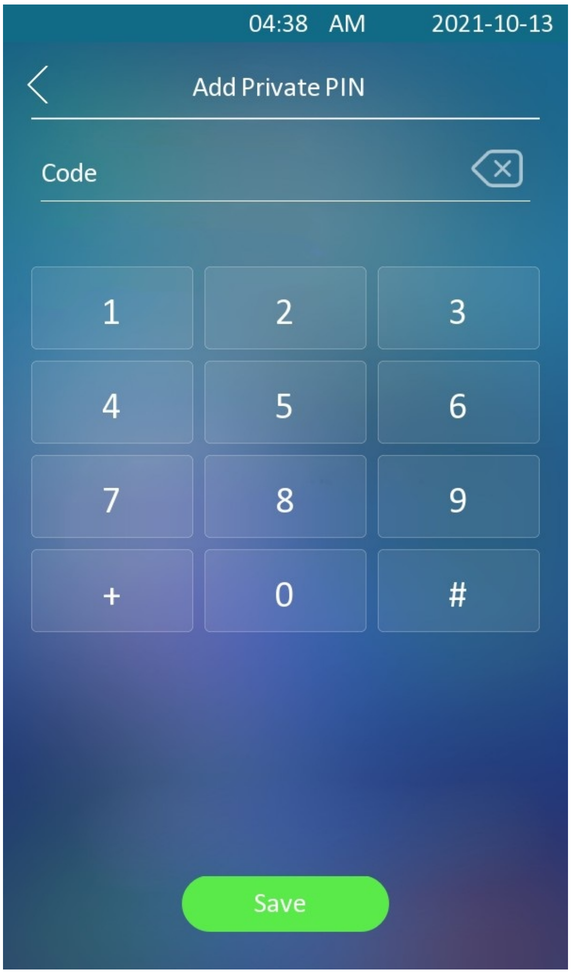
Face

Floor NO. None

* Door Door A

Web Relay 0

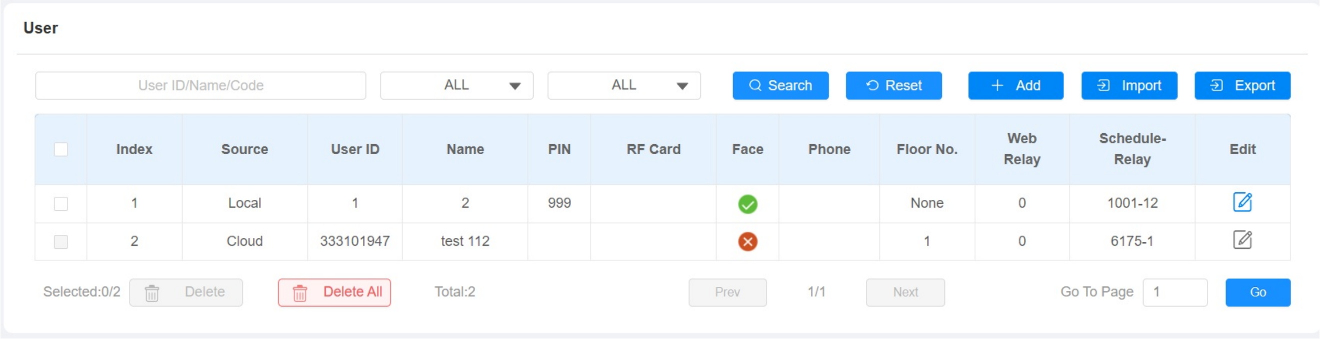
Schedule ID 1001:Always



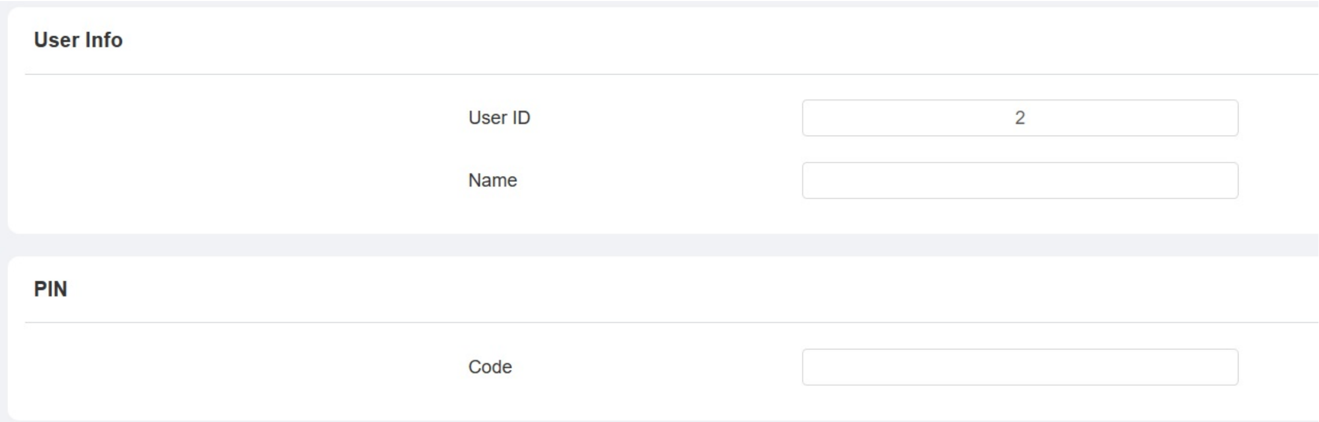
Configure Private PIN Code on the Web Interface

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.

Path: **Directory > User.**



□	Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
□	1	Local	1	2	999		✓		None	0	1001-12	✎
□	2	Cloud	333101947	test 112			✗		1	0	6175-1	✎



User Info

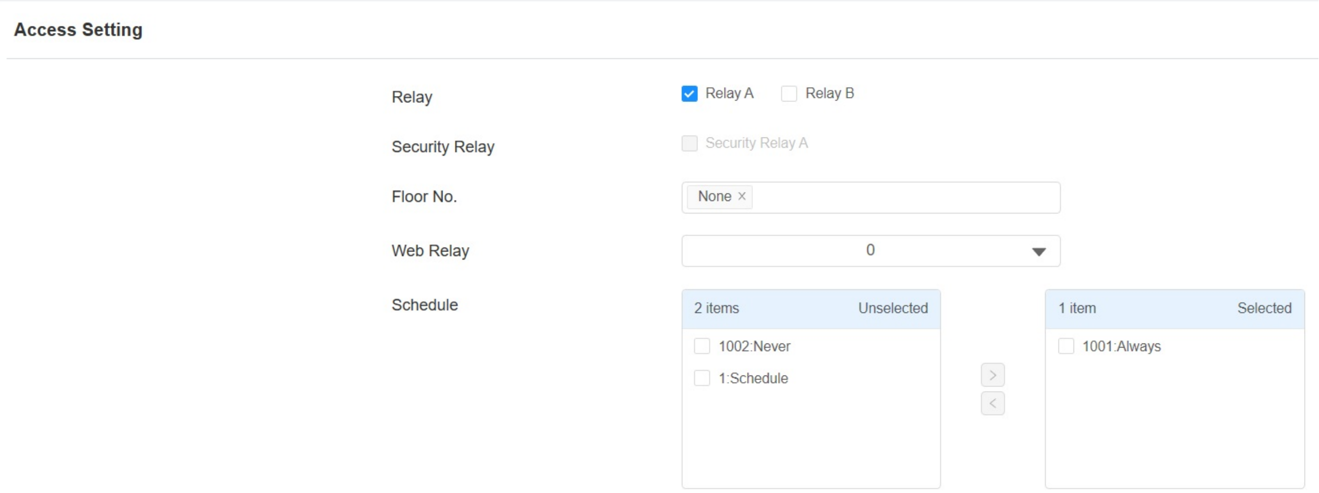
User ID: 2

Name:

PIN

Code:

After user information and PIN code are entered, you can start configuring the private PIN code for door access.



Access Setting

Relay: ☑ Relay A □ Relay B

Security Relay: □ Security Relay A

Floor No.: None ×

Web Relay: 0

Schedule:

2 items	Unselected	1 item	Selected
□ 1002:Never		□ 1001:Always	
□ 1:Schedule			

Parameter Set-up:

- **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 right box and move the one to be applied to the user(s)-specific PIN code door access to the box on the right side.

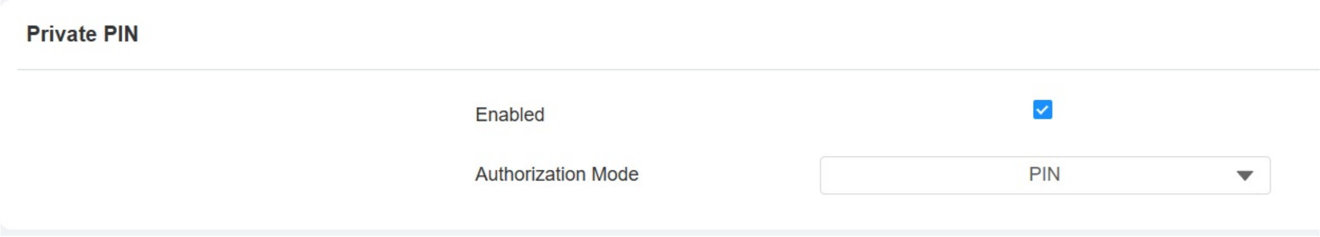
Note

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

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.

Path: **Access Control > PIN Setting > Private PIN**



Private PIN

Enabled ☑

Authorization Mode: PIN

Parameter Set-up:

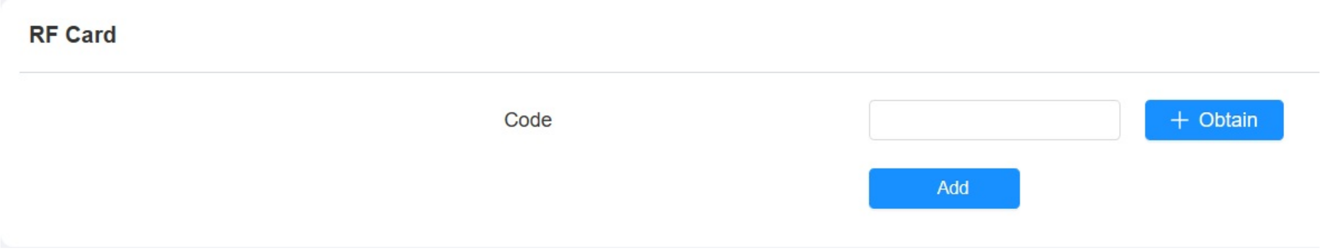
- **Authorization Mode:** select access mode between **PIN** and **APT#+PIN.** If you select **PIN**, then you are only required to enter the PIN code directly for the door access, while if you select **APT#+PIN**, then you are required to enter the Apartment Number first before entering your PIN code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

Configure RF Card for Door Unlock

You can add RF card for the specific user for the door unlock on the web interface and on the device.

Configure RF Card on the Web Interface

You can tap the RF card on the reader and click obtain to add RF card for the user. Path: **Directory > User > RF Card.**



RF Card

Code

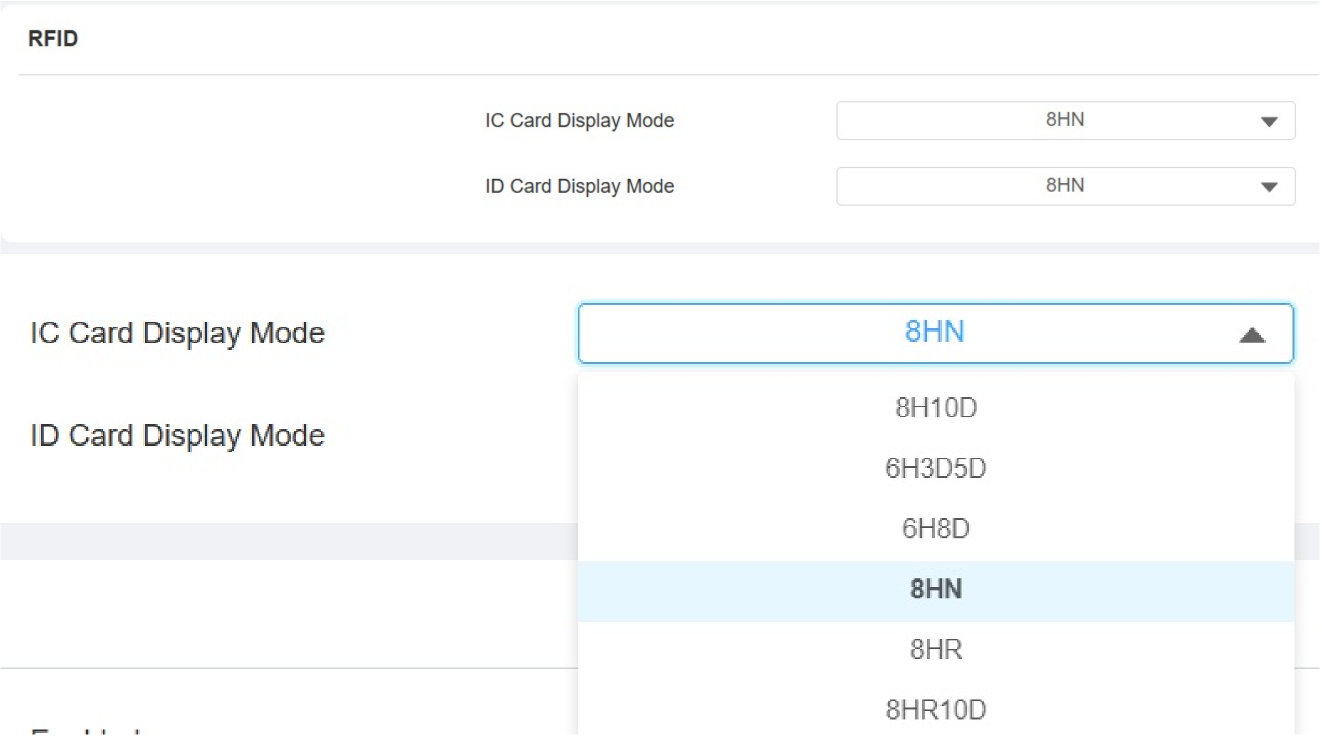
Note

- 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 the door access.

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.

Path: **Access Control > Card setting >RFID.**



RFID

IC Card Display Mode: 8HN

ID Card Display Mode: 8HN

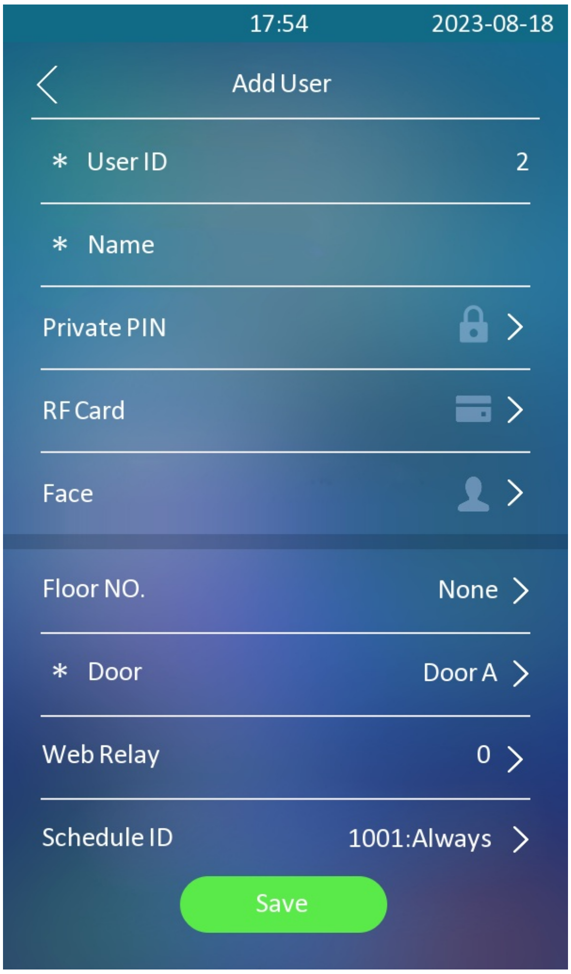
Parameter Set-up:

- **IC/ID Card Display Mode**: select the card format for the **ID/IC Card** for the door access among six format options: **8H10D; 6H3D5D; 6H8D; 8HN; 8HR; 8HR10D**. The card code format is **8HN** by default in the door phone.

Configure Facial Recognition for Door Unlock

Configure Facial Recognition on the Device

You can configure door access by facial recognition on the device by entering the user's name and registering your facial ID on the device for door access. Path: **User > User List > Add User.**



17:54 2023-08-18

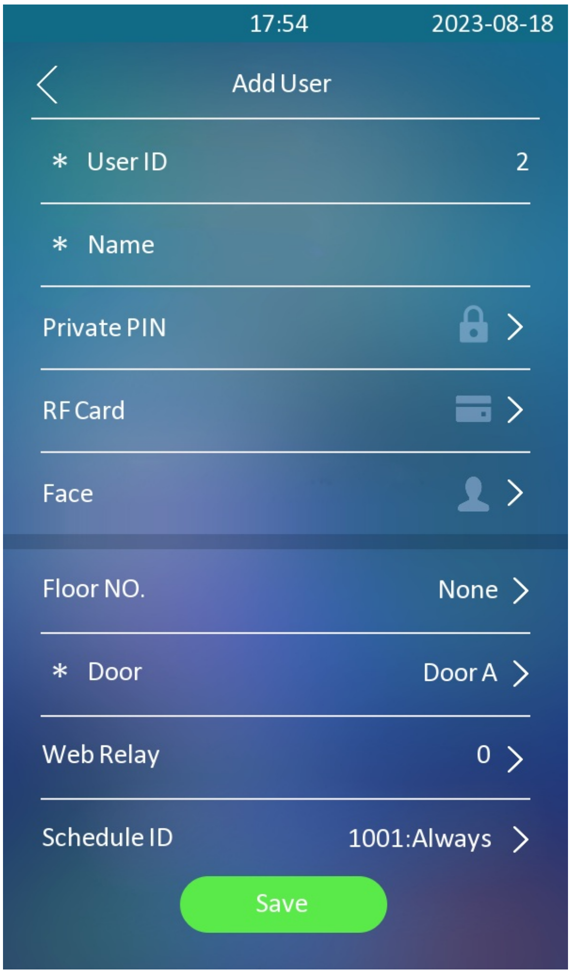
Add User

* User ID	2
* Name	
Private PIN	
RF Card	
Face	
Floor NO.	None
* Door	Door A
Web Relay	0
Schedule ID	1001:Always

Upload Face Data on the Device

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

Path: **User > User List > Add User.**



17:54 2023-08-18

Add User

* User ID 2

* Name

Private PIN

RF Card

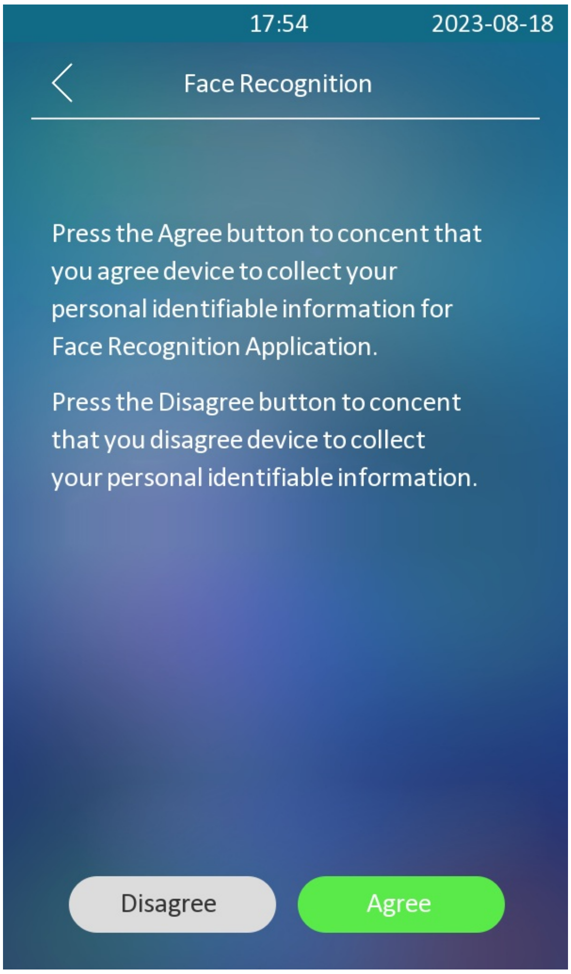
Face

Floor NO. None

* Door Door A

Web Relay 0

Schedule ID 1001:Always

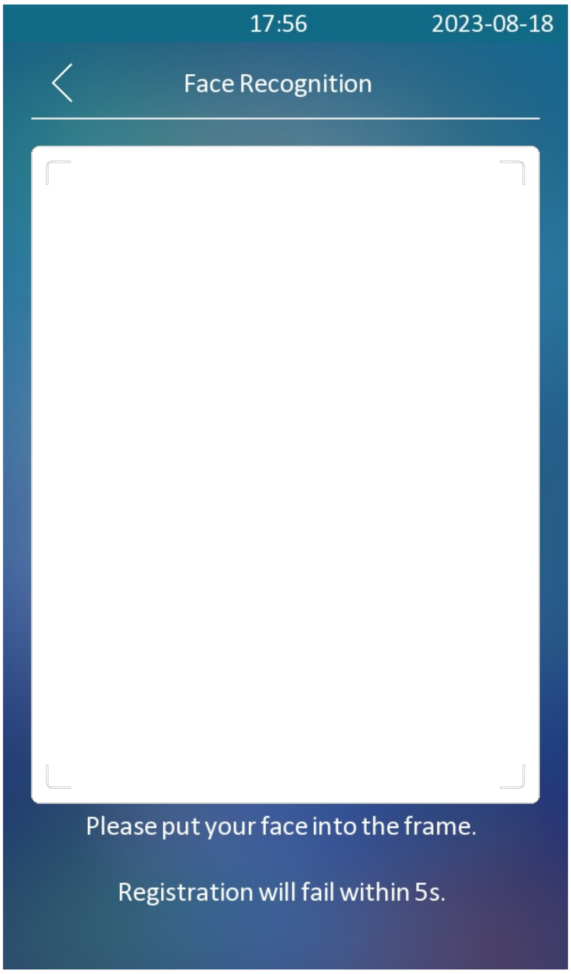


17:54 2023-08-18

Face Recognition

Press the Agree button to concent that you agree device to collect your personal identifiable information for Face Recognition Application.

Press the Disagree button to concent that you disagree device to collect your personal identifiable information.



17:56 2023-08-18

Face Recognition

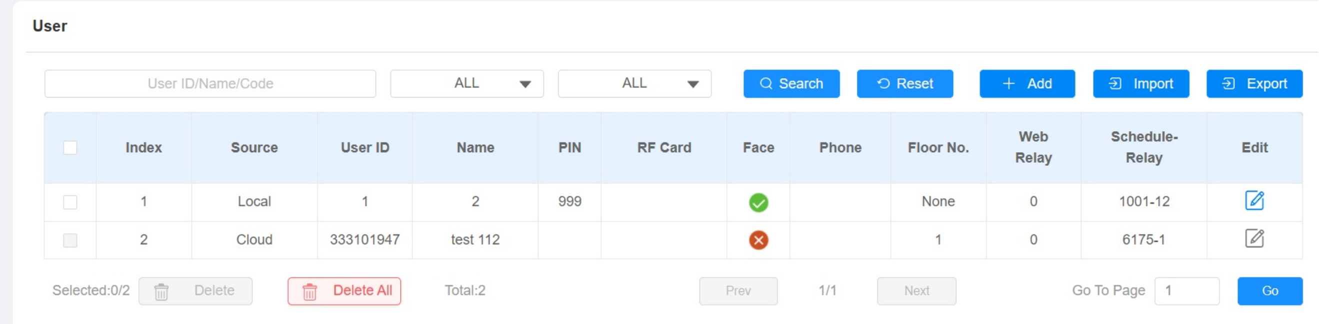
Please put your face into the frame.

Registration will fail within 5s.

Upload Face Data on the Web Interface

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

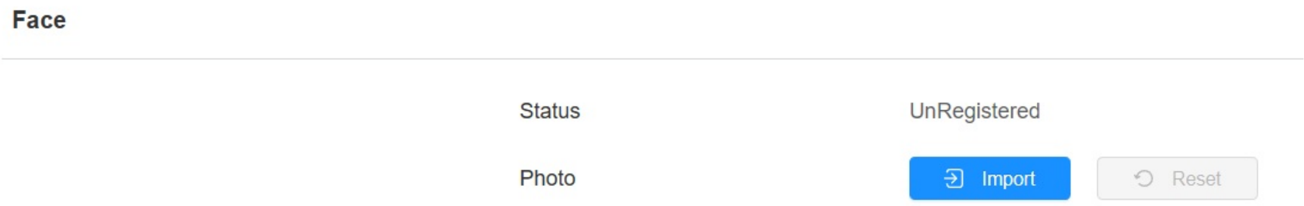
To do so, go to **Directory** > **User**, then click **+Add**. After that, upload the face photo.



User

□	Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
□	1	Local	1	2	999		✓		None	0	1001-12	✎
□	2	Cloud	333101947	test 112			✗		1	0	6175-1	✎

Selected:0/2 Total:2 1/1



Face

Status UnRegistered

Photo

Parameter Set-up:

- **Status**: it will show **Registered** when the picture uploaded conforms to the format and standard otherwise it would show **Unregistered** as the default. However, the status will be changed back to **Unregistered** if the picture uploaded is cleared when you press the **Reset** tab.
- **Photo(jpg/png)**: select the picture with jpg or png format to be uploaded to the device and press if you want to clear the picture uploaded.

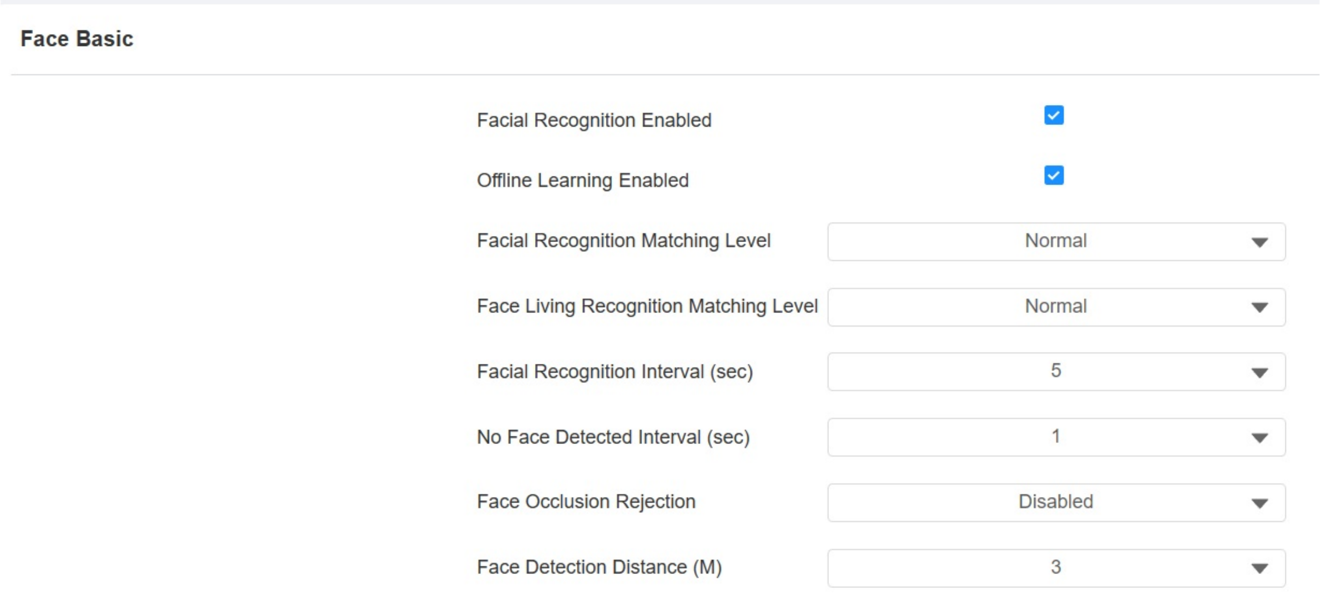
Note

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

Configure Facial Recognition

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

To configure the configuration on the web **Access Control > Face Setting** interface.



Face Basic

Facial Recognition Enabled	☑
Offline Learning Enabled	☑
Facial Recognition Matching Level	Normal
Face Living Recognition Matching Level	Normal
Facial Recognition Interval (sec)	5
No Face Detected Interval (sec)	1
Face Occlusion Rejection	Disabled
Face Detection Distance (M)	3

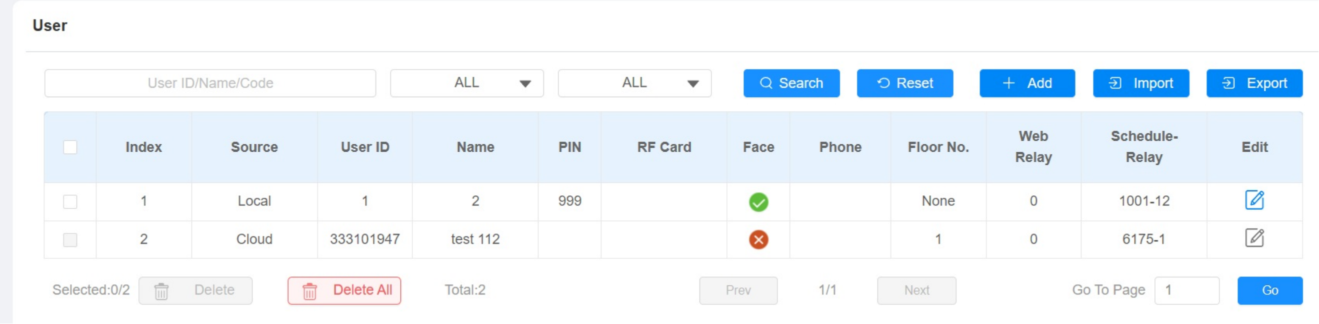
Parameter Set-up:

- **Offline Learning Enabled**: select **Enable** 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.

- **Facial Recognition Matching Level**: 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 or in another way around in facial recognition.
- **Face Living Recognition Matching Level**: select an 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 the time interval between every two facial recognitions from 1-8 seconds. For example, if you select **5** then you have to wait for 5 seconds. Before you are allowed to perform the facial recognition again.
- **No Face Detected Interval(Sec)**: set a valid time interval for the passed body temperature authentication. If the time interval is too long, it might be taken advantage by others to gain door entry through face recognition only. For example, if you passed the body temperature detection but failed in the face recognition, then you walked away, and someone behind you might try using only the face recognition for the door entry before reaching the valid time interval. So you can shorten the time interval to anywhere from 1-8 seconds so that no one can gain door entry with face recognition only. And this would also help speed up the quick door entry as the door phone will quickly return to the home screen for temperature detection when anyone failed in face recognition.
- **Face Detection Distance(M)**: you set the valid distance for face detection (1-meter, 2-meter, and 3 meters). For example, if you want to reduce the number of unnecessary face recognition of the people who happens to walk past the device. The default distance is 3 meters.

Configure Door Access Using Configured Files

E18 allows you to speedily configure user(s)-specific door access in batch by importing the configured all-in-one door access control files incorporating user information, door access type, door access schedule, etc., thus all the door access setting can be done at one stop, saving your time and effort from configuring the door access for users separately when users are large in number. Path: **Directory > User > User.**



User

User ID/Name/Code | ALL ▾ | ALL ▾ | Search | Reset | + Add | Import | Export

□	Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
□	1	Local	1	2	999		✓		None	0	1001-12	✎
□	2	Cloud	333101947	test 112			✗		1	0	6175-1	✎

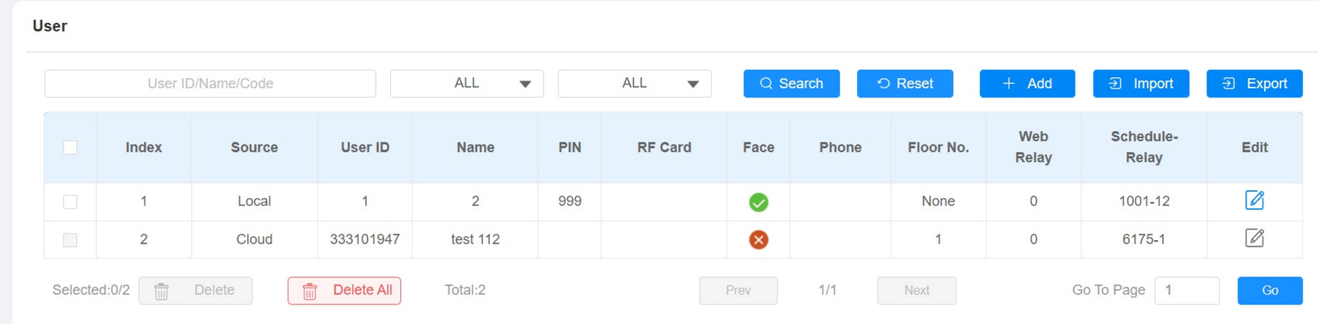
Selected:0/2 | Delete | Delete All | Total:2 | Prev | 1/1 | Next | Go To Page 1 | Go

Note

- Configured files for facial recognition and the other types of configured door access files are separated with different file forms.

Edit the User(s)-specific Door Access Data

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



User

User ID/Name/Code | ALL ▾ | ALL ▾ | Search | Reset | + Add | Import | Export

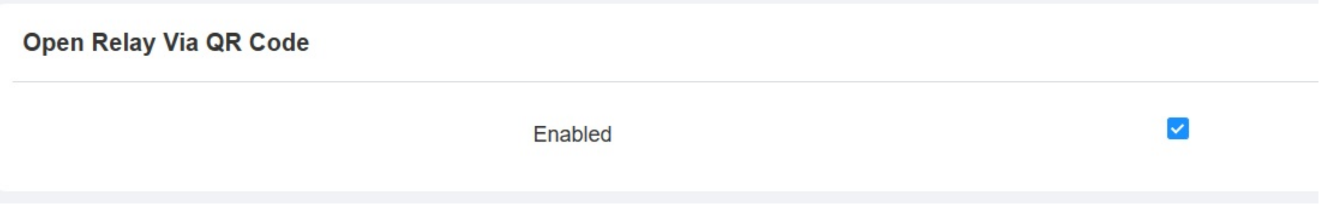
□	Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
□	1	Local	1	2	999		✓		None	0	1001-12	✎
□	2	Cloud	333101947	test 112			✗		1	0	6175-1	✎

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

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.

Path: **Access Control > Relay > Open Relay via QR Code.**



Open Relay Via QR Code

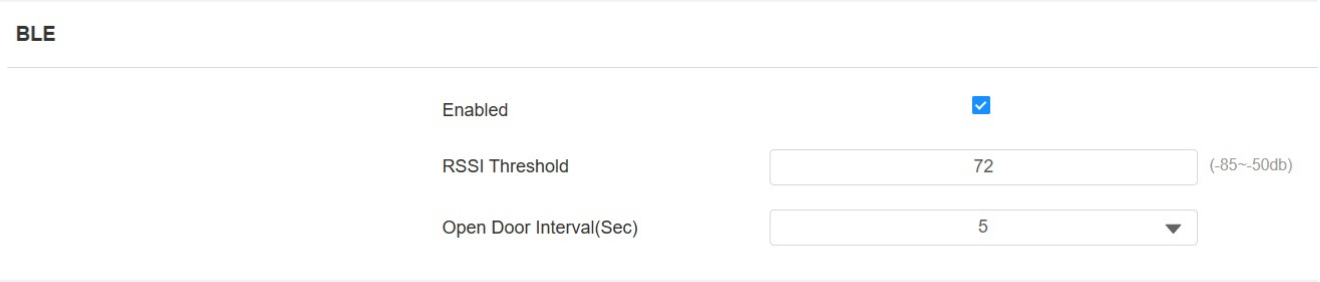
Enabled ☑

> **Note**
>
> - The function should work with Akuvox cloud. For more information, please contact Akuvox technical team.

Unlock by Bluetooth

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.

Path: **Access Control > BLE > BLE.**



BLE

Enabled ☑

RSSI Threshold 72 (-85~-50db)

Open Door Interval(Sec) 5

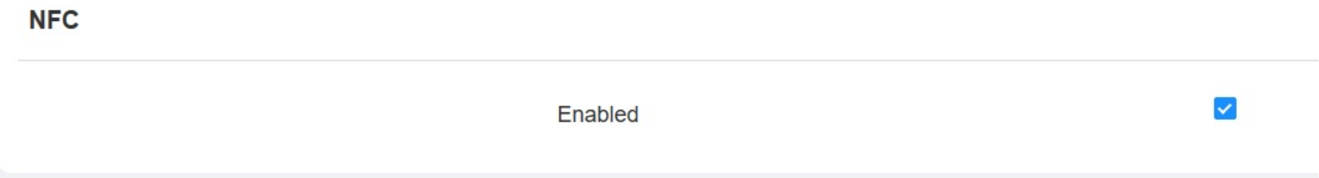
Parameter Set-up:

- **RSSI Threshold**: select the signal receiving strength from -85~-50db in absolute terms. The higher value 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.

Unlock by NFC

NFC (Near Field Communication) is a popular way for door access. It uses radio waves for data transmission interaction. The device can be unlocked by NFC. You can keep the mobile phone closer to the device for door access.

Path: **Access Control > Card Setting> NFC**



NFC

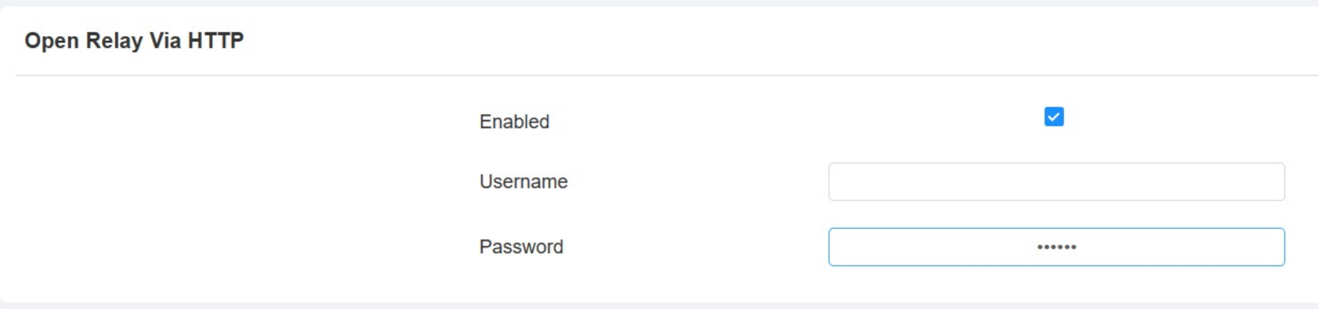
Enabled ☑

Unlock by HTTP Command on Web Browser

The door phone supports remote door unlocking via an HTTP command. Simply enable this feature and input the HTTP command (URL) for the door phone. This will trigger the relay and open the door, even if the users are away from the device.

Path: **Access Control > Relay**

- **Open Relay via HTTP**



Open Relay Via HTTP

Enabled ☑

Username

Password ••••••

Parameter Set-up:

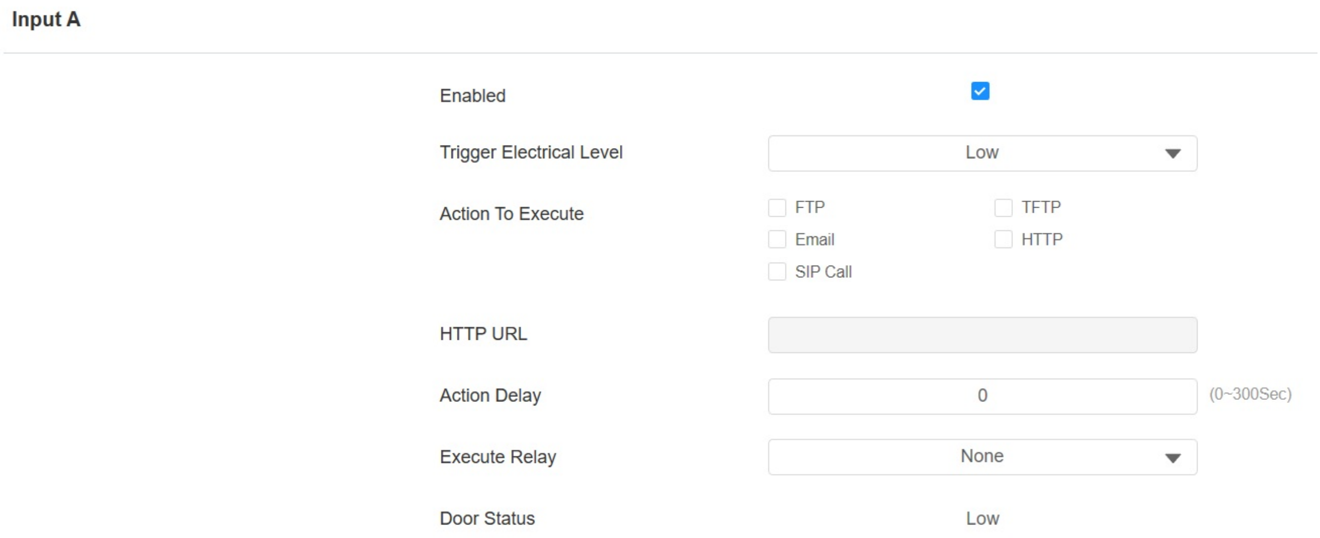
- **User Name**: enter the user name of the device web interface, for example, **admin.**
- **Password**: enter the password for the HTTP command. For example, **12345.**

Please refer to the following example: http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

Unlock by Exit Button by the Door

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.

Path: **Access Control > Input > Input A**



Input A

Enabled	☑
Trigger Electrical Level	Low ▾
Action To Execute	□ FTP □ TFTP □ Email □ HTTP □ SIP Call
HTTP URL	
Action Delay	0 (0~300Sec)
Execute Relay	None ▾
Door Status	Low

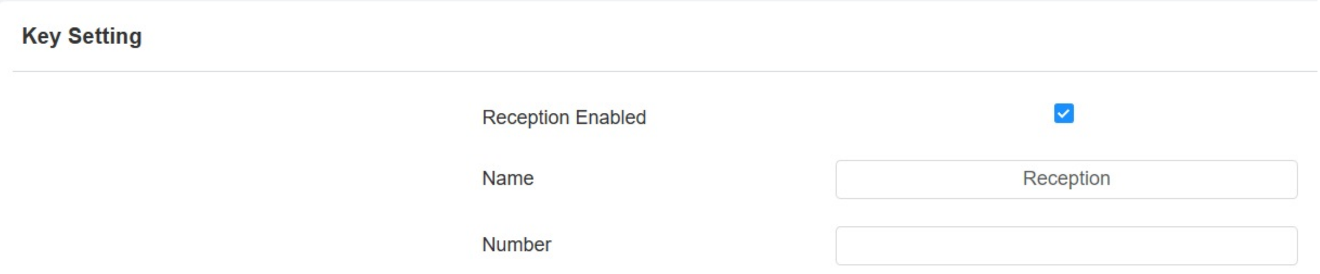
Parameter Set-up:

- **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 five options: **FTP, Email, TFTP, HTTP**, and **SIP Call.**
- **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 your press the button.

Unlock by Reception Tab

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.

Path: **Intercom > Basic > Key Setting**



Key Setting

Reception Enabled	☑
Name	Reception
Number	

Parameter Set-up:

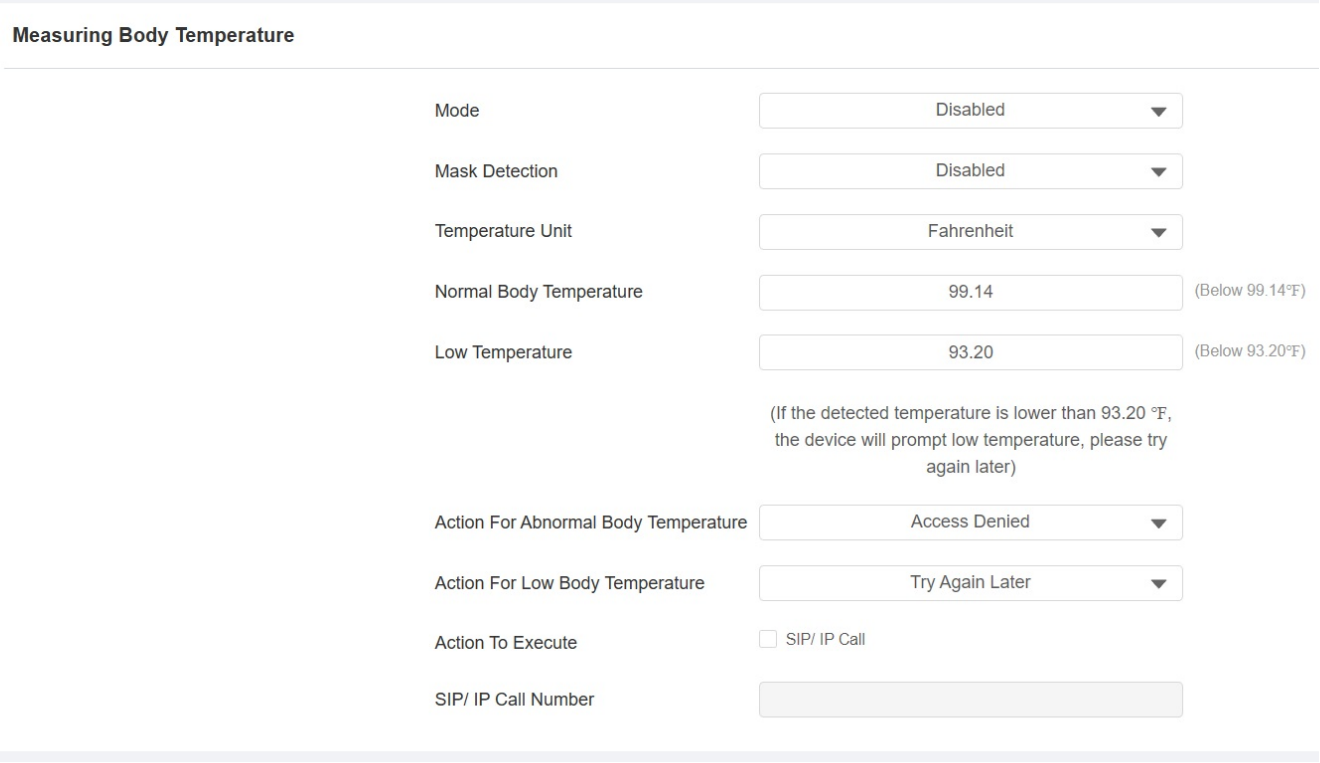
- **Number**: enter the SIP/IP number to be called after pressing the **Reception icon** for door access.

Body Temperature Measurement for Door Access

The body temperature measurement function allows the door phone measures body temperature and checks masks for safety. When enabled, the door phones only opens the door for residents or visitors who pass the test.

Body Temperature Measurement Configuration

You can configure the body temperature measurement function in terms of defining the normal temperature as well as making schedule for the validity of the function etc. Path: **Access Control > Body Temperature > Measuring Body Temperature.**



Measuring Body Temperature

Mode	Disabled ▼	
Mask Detection	Disabled ▼	
Temperature Unit	Fahrenheit ▼	
Normal Body Temperature	99.14	(Below 99.14℉)
Low Temperature	93.20	(Below 93.20℉)
	(If the detected temperature is lower than 93.20 ℉, the device will prompt low temperature, please try again later)	
Action For Abnormal Body Temperature	Access Denied ▼	
Action For Low Body Temperature	Try Again Later ▼	
Action To Execute	□ SIP/ IP Call	
SIP/ IP Call Number		

Parameter Set-up:

- **Mode**: select either **Disabled Mode, Wrist Mode**, or **Forehead Mode** for temperature measurement according to your need. The device can be installed with a digital forehead temperature detector therefore you can are required to set the mode properly according to your application.
- **Mask Detection**: select **Disable** if you want to turn off the mask detection. Select **Set mask-wearing** as mandatory and the device will check if the visitor is wearing a mask or

not while reminding the visitor with the announcement "Please wear a mask". Select **Display mask-wearing** prompt and the device will display the mask- wearing prompt only without making the mask-wearing mandatory.

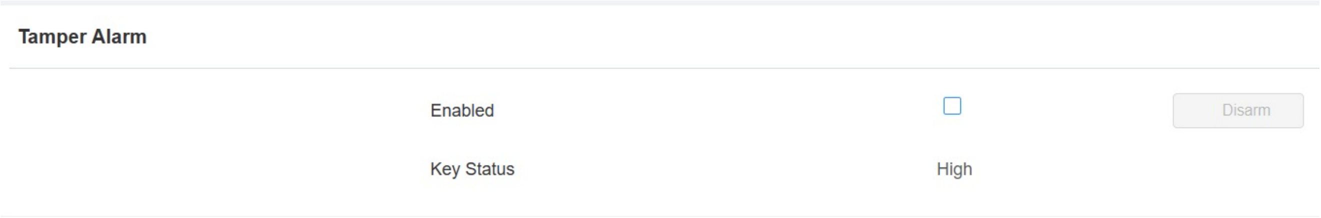
- **Normal Body Temperature**: set the body temperature to the predefined body temperature as the measuring basis in either **Fahrenheit** or **Celsius**. For example, if you set the temperature at 37.3 degrees celsius as the normal temperature, then any body temperature measured higher than 37.3 degrees celsius will be deemed as an abnormal temperature, while a temperature is lower than 34 degrees celsius will be deemed as low body temperature.
- **Action For Abnormal Body Temperature**: if you select **Access Denied** then anyone who is detected with abnormal body temperature will be denied door access. If you select **Just For Reminder** then anyone with abnormal body temperature will still be granted door access.
- **Action for Low Body Temperature**: if **Try Again Later** is selected, you will be denied the door access with the prompt "Try again later for the low body temperature". If you select **Just For Reminder**, then anyone with low body temperature will still be granted door access.
- **Action to Execute**: check the box to enable or disable the SIP/IP Call. If you want to be notified via SIP/IP call when abnormal temperature and low temperature are detected.
- **SIP/IP Call Number**: enter the SIP or IP call for the notification. The field will appear for you to fill in SIP/IP numbers when you check the **Action to Execute** box.

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.

Path: **System > Security > Tamper Alarm**



Tamper Alarm

Enabled	□	Disarm
Key Status	High	

Parameter Set-up:

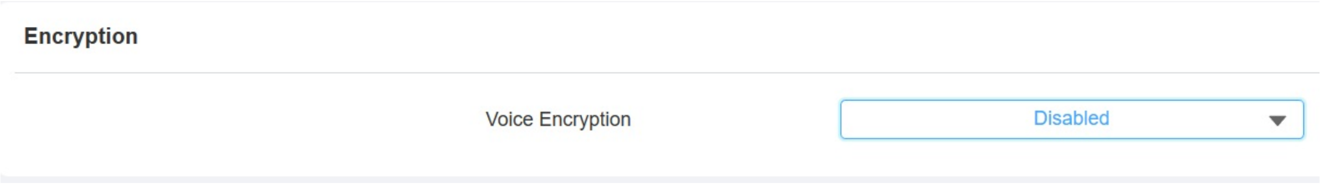
- **Enabled**: tick the check box to enable the tamper alarm function. When the tamper alarm goes off, you can press the **Disarm** tab beside the check box to clear the alarm.
- **Key Status**: tamper alarm will not be triggered unless the key status is shifted from **Low** to **High** status.

> **Note**
>
> - **Disarm** tab will turn gray when the tamper alarm is cleared.
> - The round rubber button at the back of the device must be in press-down status otherwise the alarm will not be fired.

Voice Encryption

Secure Real-time Transport Protocol (SRTP) is a protocol derived from the Real-time Transport Protocol (RTP). It enhances the security of data transmission by providing encryption, message authentication, integrity assurance, and replay protection.

Path: **Account** > **Advanced** > **Encryption** interface.



Encryption

Voice Encryption	Disabled ▾

Parameter Set-up:

- **Voice Encryption(SRTP)**: choose **Disabled, Optional** or **Compulsory** for SRTP. If it is **Optional** or **Compulsory**, the voice during the call is encrypted, and you can grab the RTP packet to view.

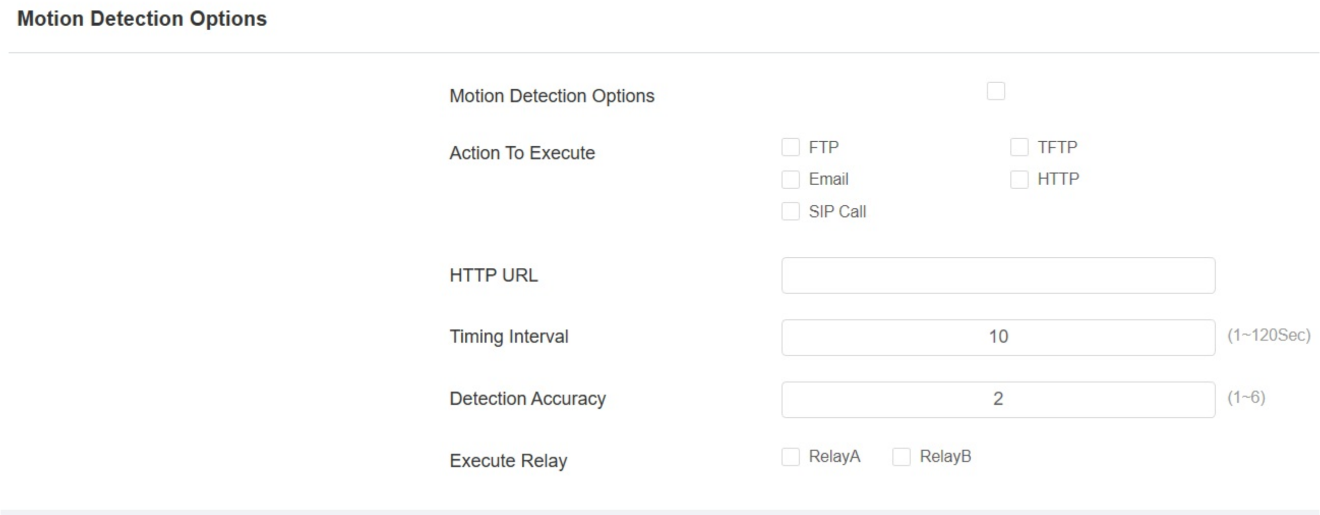
Motion Detection

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 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.

Path: **Surveillance** > **Motion** > **Motion Detection Options** interface.



Motion Detection Options

Motion Detection Options	□	
Action To Execute	□ FTP □ Email □ SIP Call	□ TFTP □ HTTP
HTTP URL		
Timing Interval	10	(1~120Sec)
Detection Accuracy	2	(1~6)
Execute Relay	□ RelayA □ RelayB	

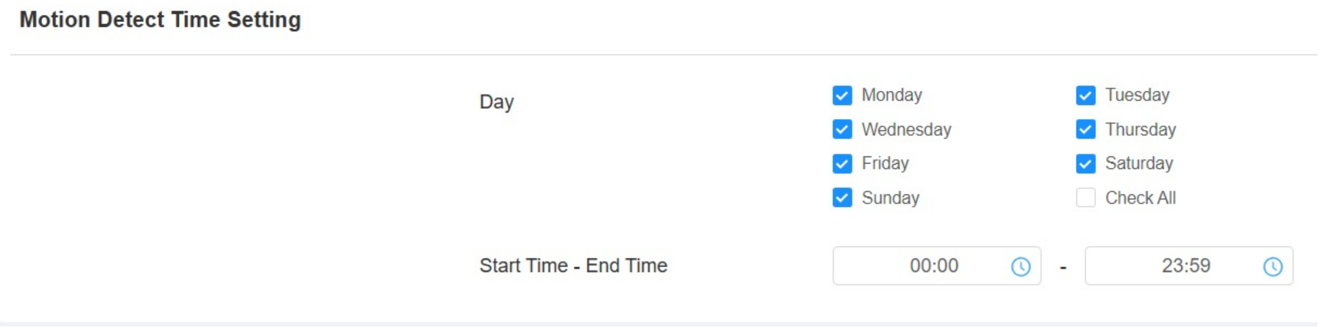
Parameter Set-up:

- **Action to Execute**: select the action to be executed (FTP, TFTP, Email, HTTP, and SIP

Call) after motion detection is triggered.

- **HTTP URL**: enter the HTTP URL command which will be sent to the designated server for a certain action.
- **Time Interval**: set the time interval in the same way as you do on the device.
- **Detection Accuracy**: set the detection accuracy for the detection sensitivity. The higher value is, the greater sensitivity. The default detection accuracy value is **2**.
- **Execute Relay**: select relay A or relay B to be triggered when the motion detection is triggered.

You can also set the motion detection time schedule.



Motion Detect Time Setting

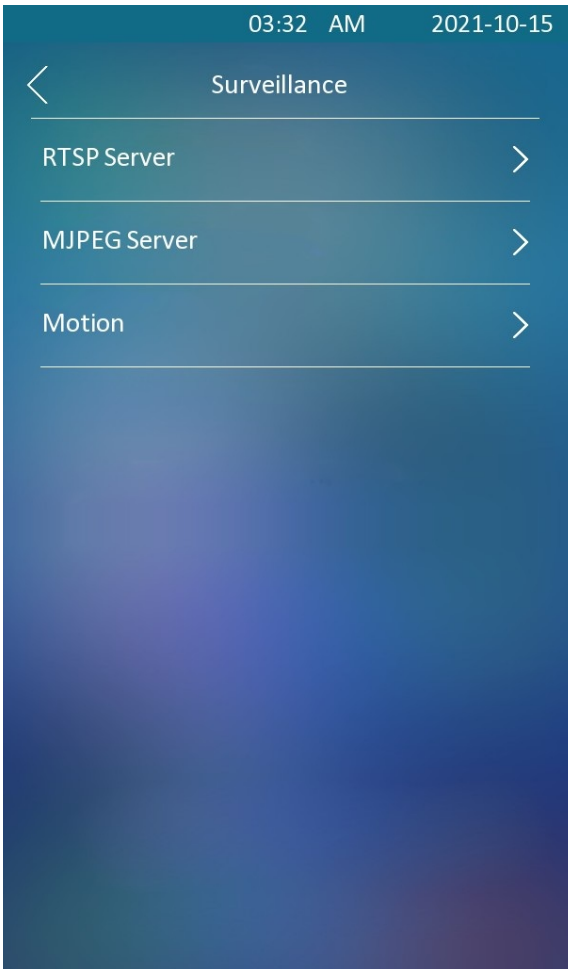
Day

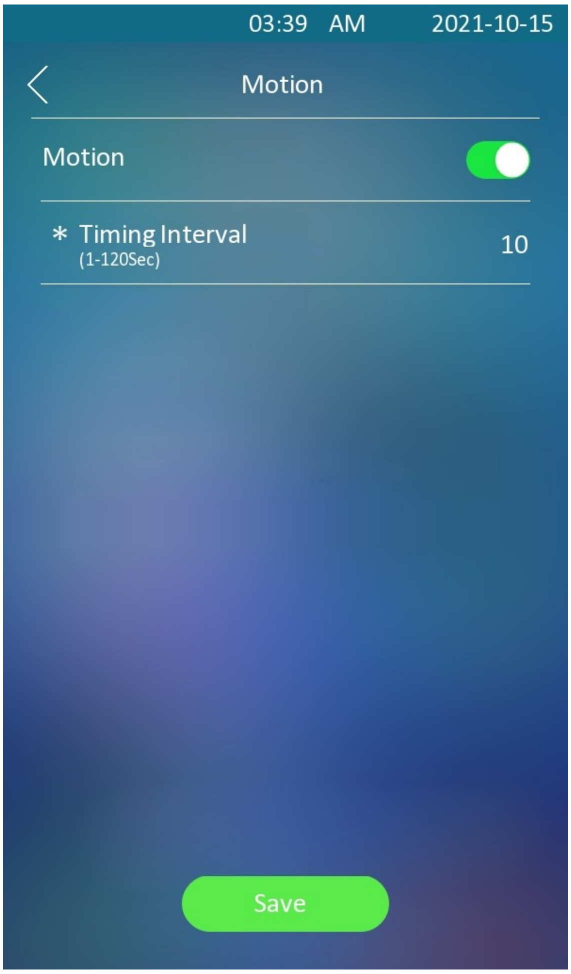
☑ Monday ☑ Tuesday
☑ Wednesday ☑ Thursday
☑ Friday ☑ Saturday
☑ Sunday □ Check All

Start Time - End Time 00:00 - 23:59

Configure Motion Detection on the Device

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





03:39 AM 2021-10-15

Motion

Motion ●

* Timing Interval (1-120Sec) 10

Save

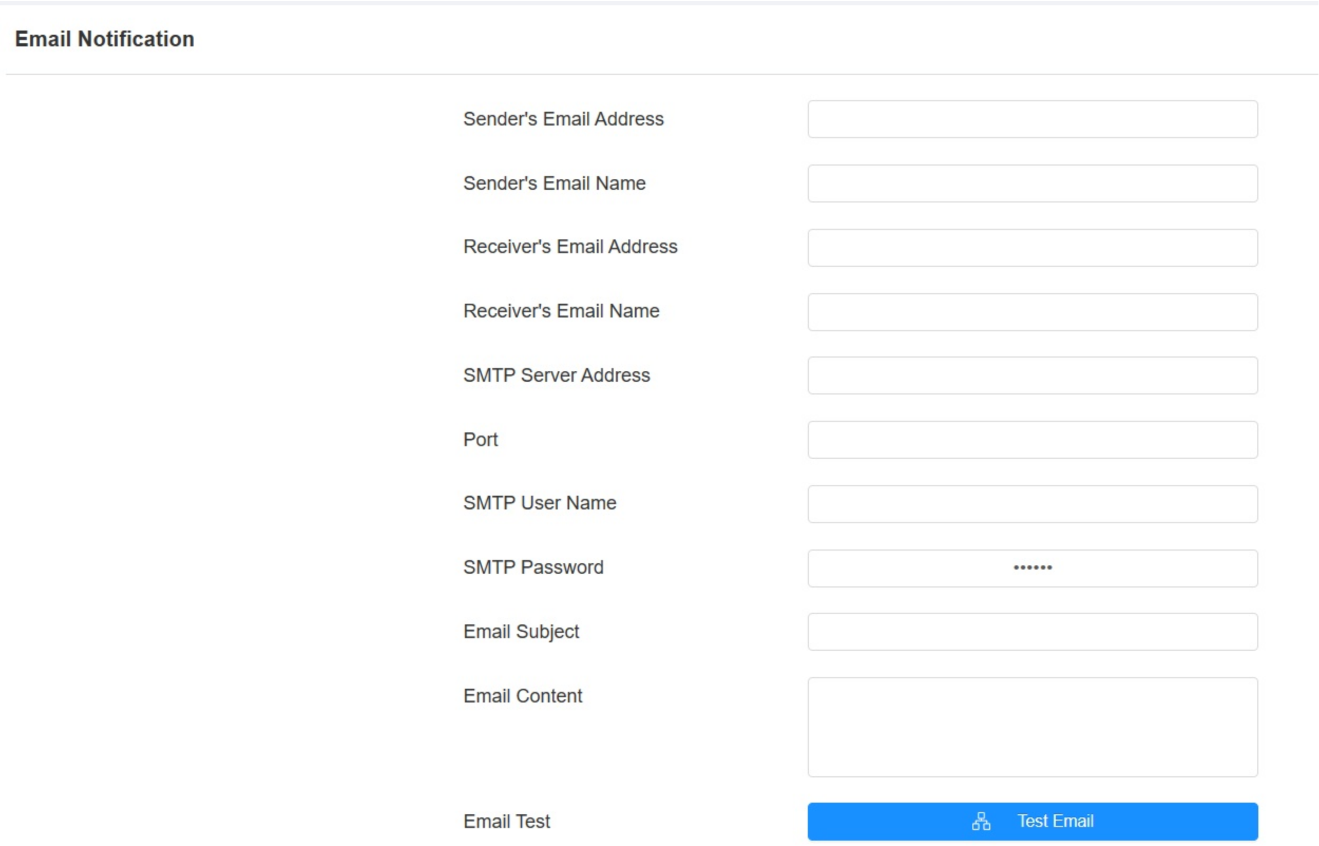
Security Notification Setting

Security notification can be initiated as an action when the motion detection is triggered. And the security notification can be made via Email, FTP server, TFTP server, and SIP call.

Email Notification Setting

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

Path: **Setting > Action.**



Email Notification

Sender's Email Address	
Sender's Email Name	
Receiver's Email Address	
Receiver's Email Name	
SMTP Server Address	
Port	
SMTP User Name	
SMTP Password	••••••
Email Subject	
Email Content	
Email Test	Test Email

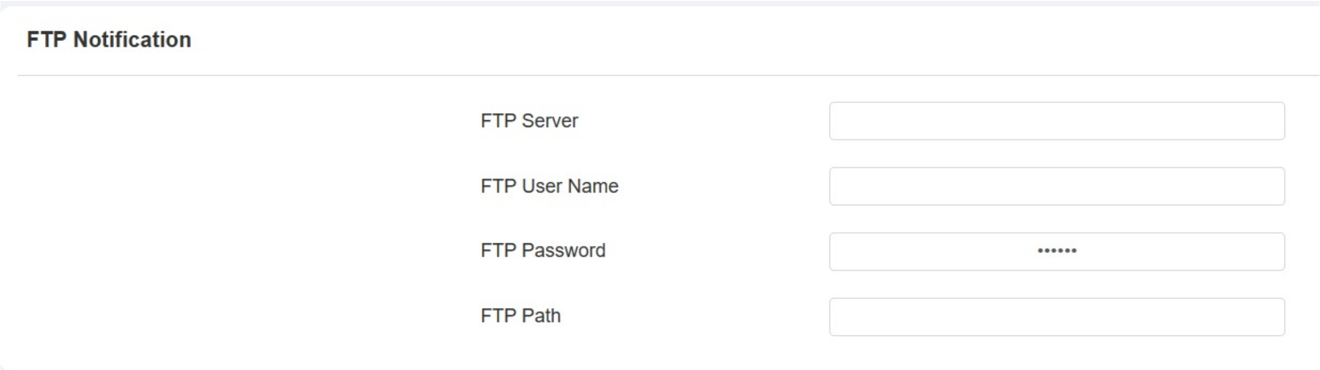
Parameter Set-up:

- **Sender's Email Name**: enter the name of the email sender.
- **Sender's Email Address**: enter the sender's email address from which the email notification will be sent out.
- **Receiver's Email Address**: enter the receiver's email address.
- **Receiver's Email Name**: enter the name of the email receiver.
- **SMTP Server Address**: enter the SMTP server address of the sender.
- **Port**: enter the port number from which the email is sent out.
- **SMTP User Name**: enter the SMTP user name, which is usually the same with the sender's email address.
- **SMTP Password**: configure the password of SMTP service, which is the same with 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.

Path: **Setting > Action > FTP Notification.**



FTP Notification

FTP Server	
FTP User Name	
FTP Password	••••••
FTP Path	

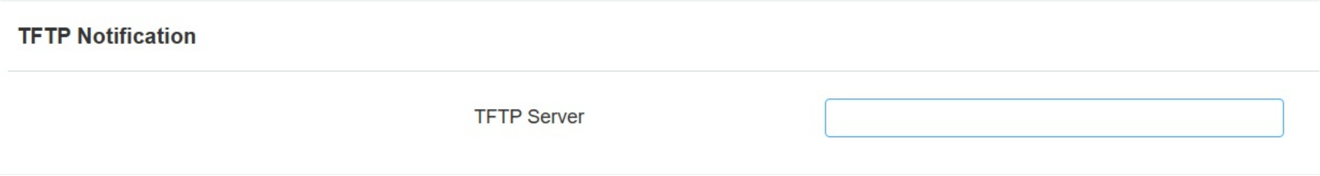
Parameter Set-up:

- **FTP Server**: enter the address (URL) of the FTP server for the FTP notification.
- **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.

Path: **Setting > Action > TFTP Notification.**



TFTP Notification

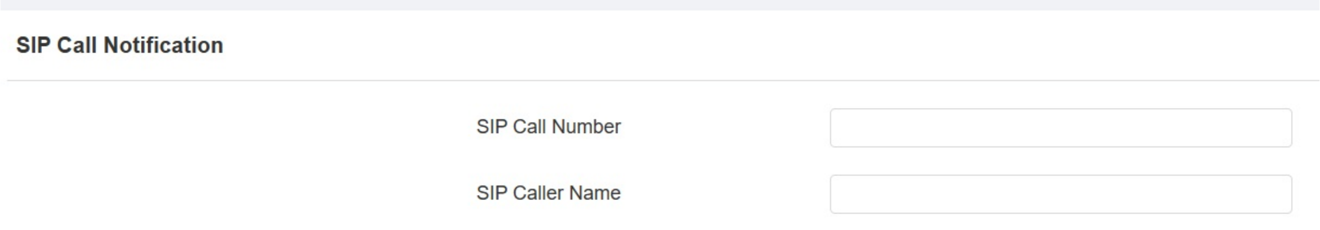
TFTP Server	

Parameter Set-up:

- **TFTP Server**: enter the address (URL) of the TFTP server for the TFTP notification.

SIP Call Notification

If you want to receive the security notification via SIP call, you can configure the FTP notification on the web interface properly. Path: **Setting > Action > SIP Call Notification.**



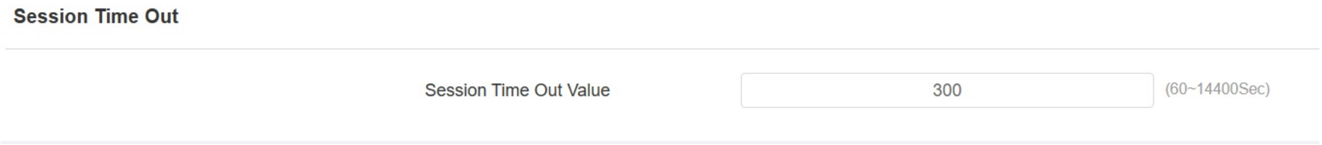
SIP Call Notification

SIP Call Number	
SIP Caller 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 set it up, go to **System> Security > Session Time Out**.



Session Time Out

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

Parameter Set-up:

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

Action URL

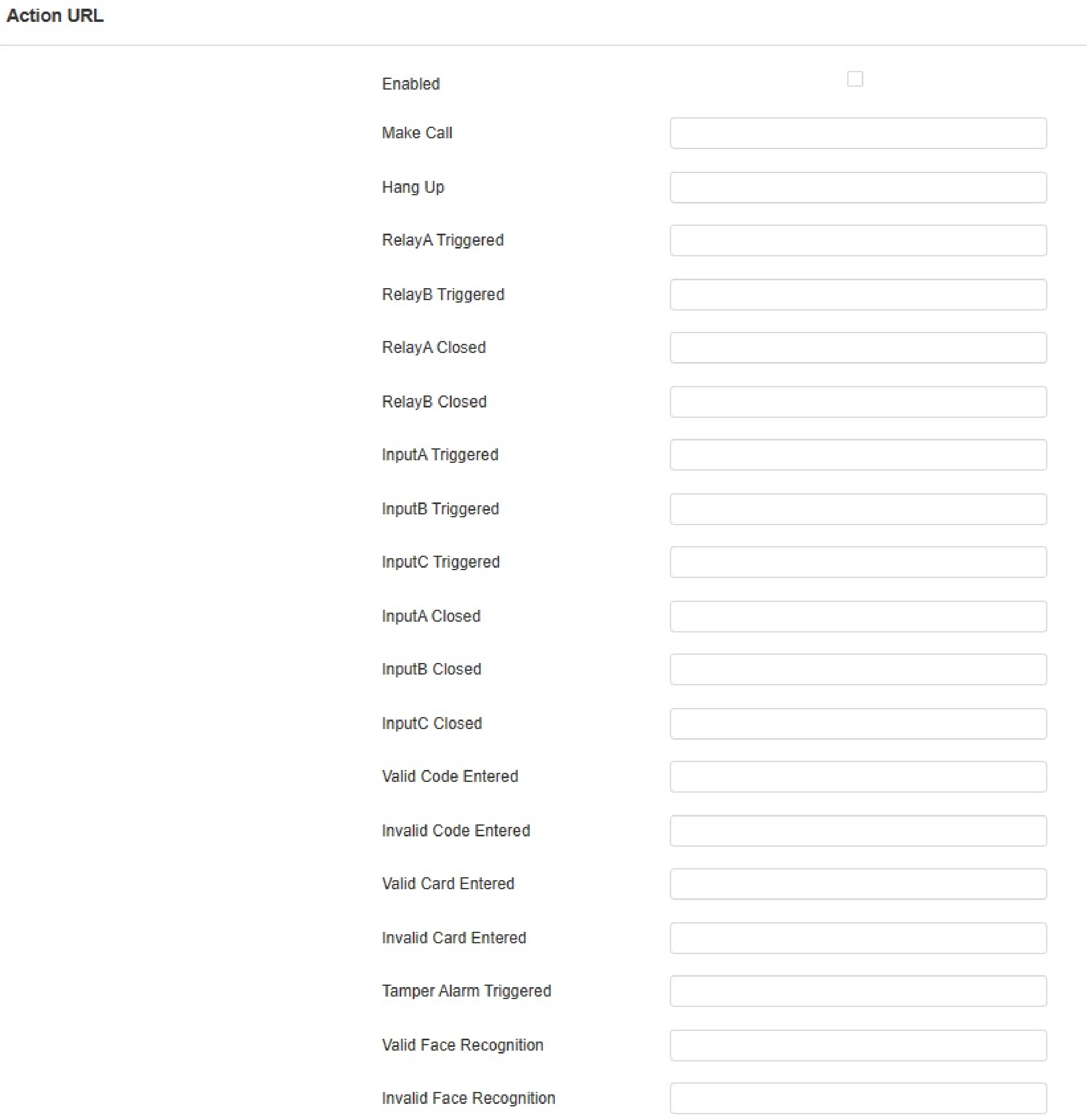
You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status, input status, PIN code, or RF card access changes.

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 **Setting > Actions URL.**



Action URL

Enabled □

Make Call

Hang Up

RelayA Triggered

RelayB Triggered

RelayA Closed

RelayB Closed

InputA Triggered

InputB Triggered

InputC Triggered

InputA Closed

InputB Closed

InputC Closed

Valid Code Entered

Invalid Code Entered

Valid Card Entered

Invalid Card Entered

Tamper Alarm Triggered

Valid Face Recognition

Invalid Face Recognition

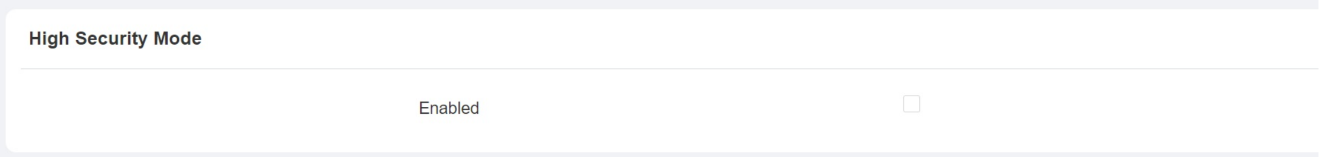
Note

- Action URL and format are provided by a third-party manufacturer, Akuvox door phone only sends the URL to third-party devices.

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 this feature on the web: **System > Security > High Security Mode**



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.

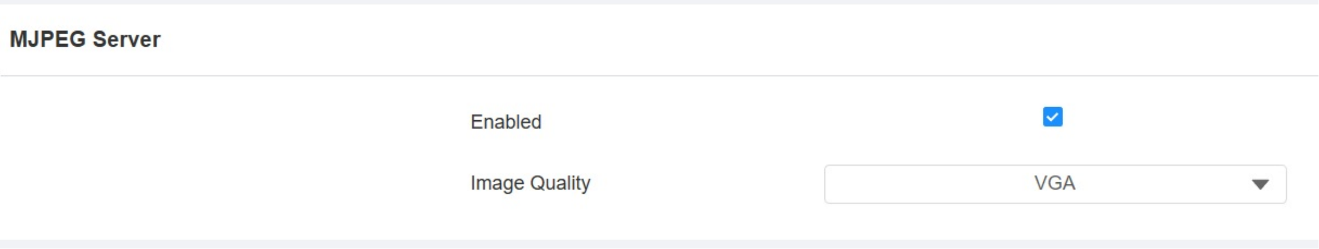
RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

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.

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.

Path: **Surveillance > MJPEG > Mjpeg Server**



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:

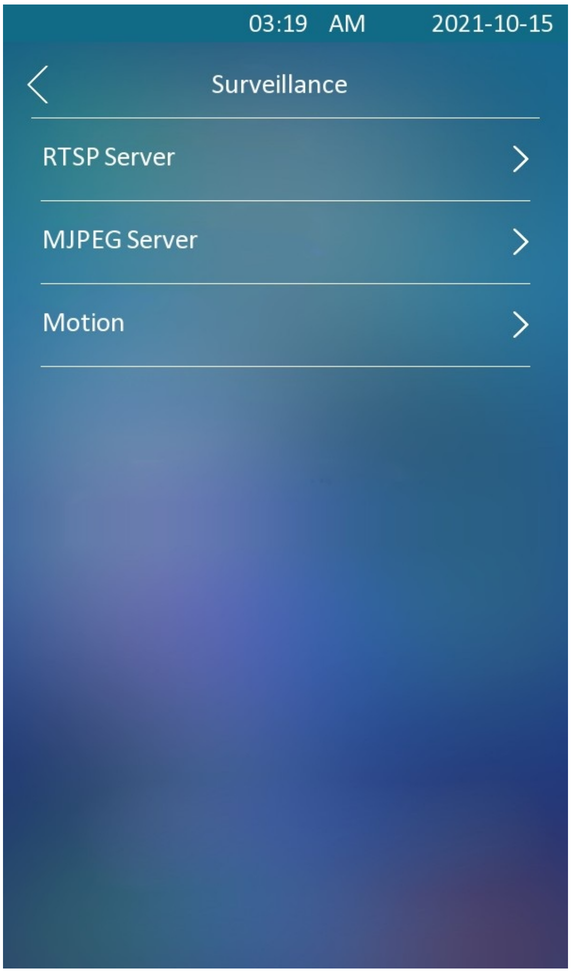
- http:// device ip:8080/picture.cgi

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

For example, if you want to capture the jpg format image of the door phone with the IP address:192.168.1.104, you can do as follows:

1. Enter http://192.168.1.104:8080/picture.jpg on the web browser
2. Press **Enter** key on your keyboard to capture the image.

You can also enable the MJPEG server on the device directly. Path: **Advanced > Surveillance > MJPEG server.**



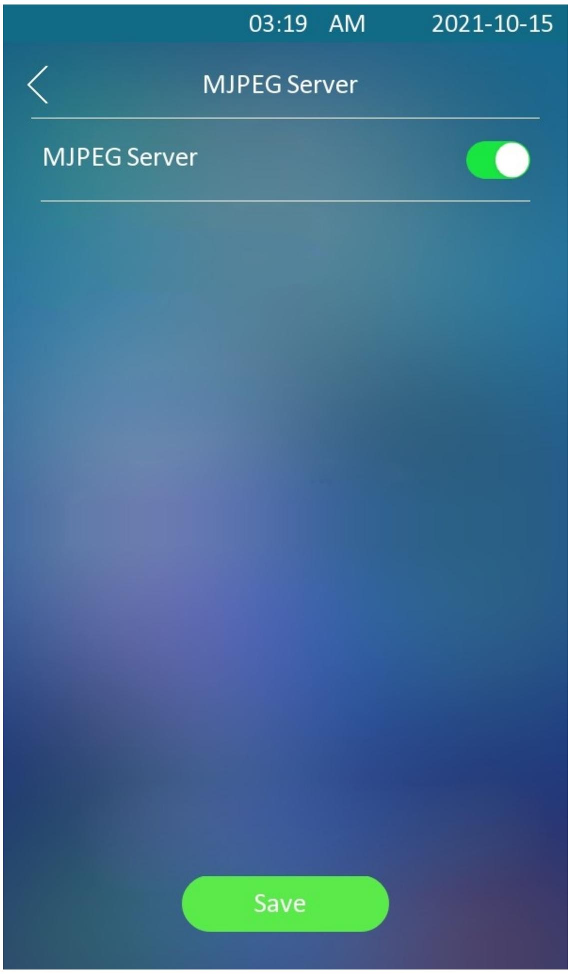
03:19 AM 2021-10-15

Surveillance

RTSP Server

MJPEG Server

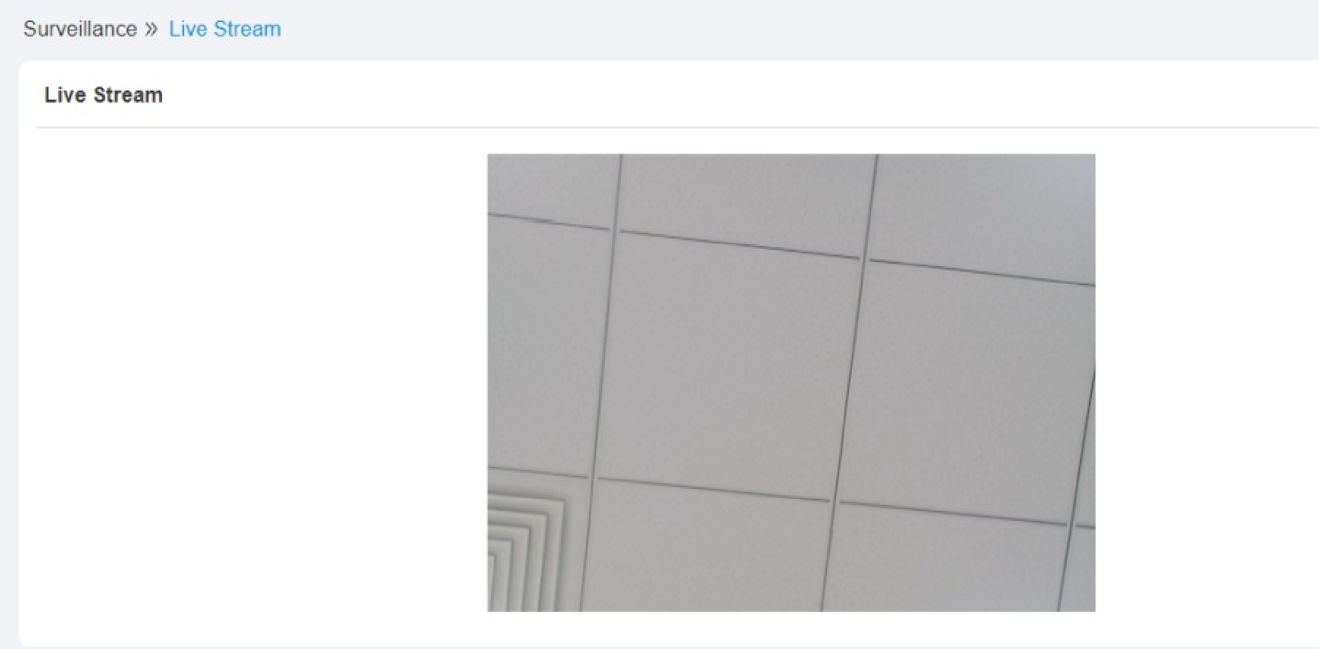
Motion



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.

Path: **Surveillance > Live Stream.**



{height="" width=""900}

Note

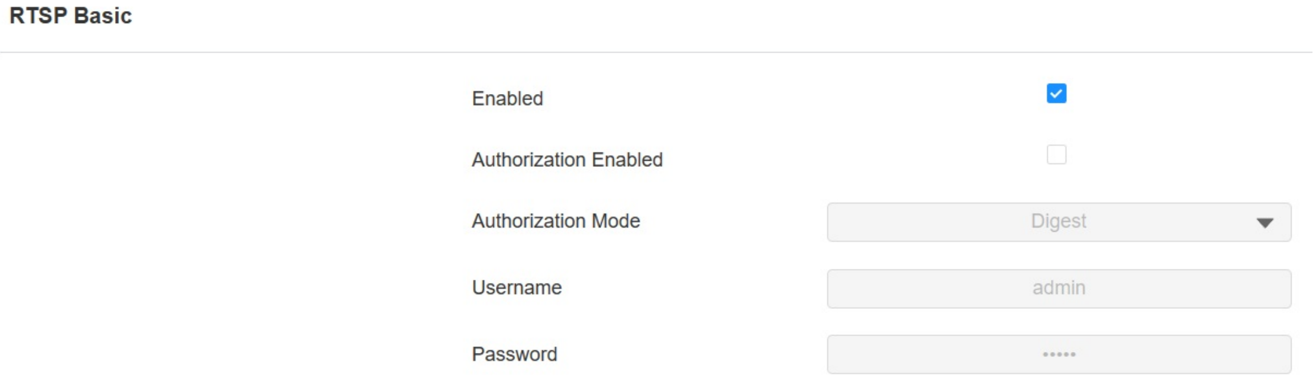
- You can also enter the correct URL (**http://IP_address:8080/video.cgi**) on the web browser if you want to obtain the real-time video directly without going to the web interface.

RTSP Stream Monitoring

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

RTSP Basic Setting

You are required to set up the RTSP function in terms of RTSP Authorization, authentication and password, etc. before you are able to use the function. Path: **Surveillance > RTSP > RTSP Basic**



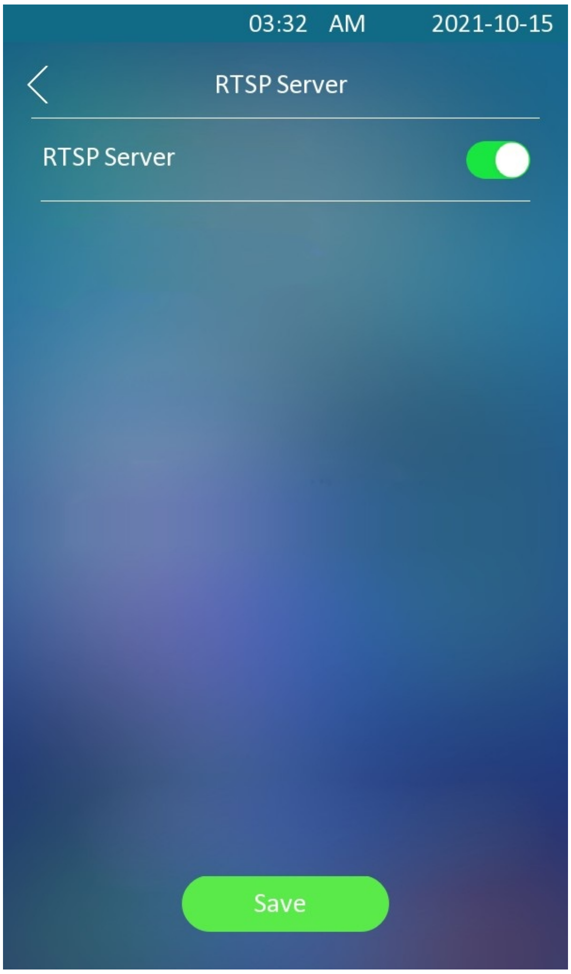
RTSP Basic

Enabled	☑
Authorization Enabled	□
Authorization Mode	Digest
Username	admin
Password	•••••

Parameter Set-up:

- **Authorization Enabled**: tick the check box to enable the RTSP authorization. If you enable the RTSP Authorization, you are required to enter RTSP Authentication Type, RTSP Username, RTSP Password on the intercom device such as an indoor monitor for authorization.
- **RTSP Authentication Type**: select RTSP authentication type between **Basic** and **Digest. Basic** is the default authentication type.

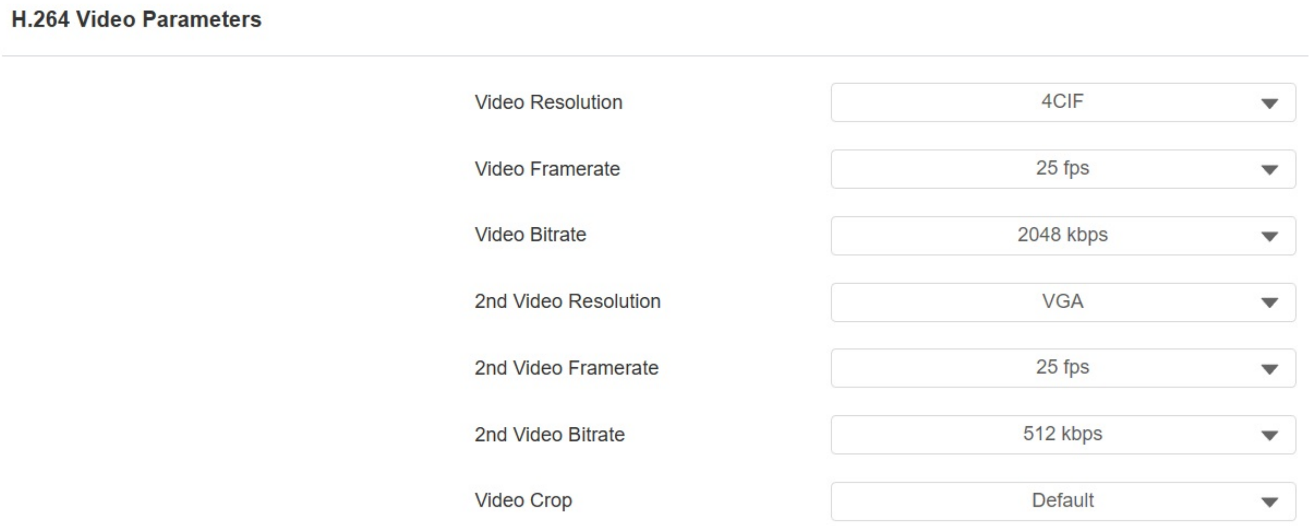
You can also enable the RTSP function on the device directly. Path: **Advanced > Surveillance > RTSP Server**



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.

Path: **Surveillance > RTSP > H.264 Video Parameters**



H.264 Video Parameters

Video Resolution	4CIF
Video Framerate	25 fps
Video Bitrate	2048 kbps
2nd Video Resolution	VGA
2nd Video Framerate	25 fps
2nd Video Bitrate	512 kbps
Video Crop	Default

Parameter Set-up:

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

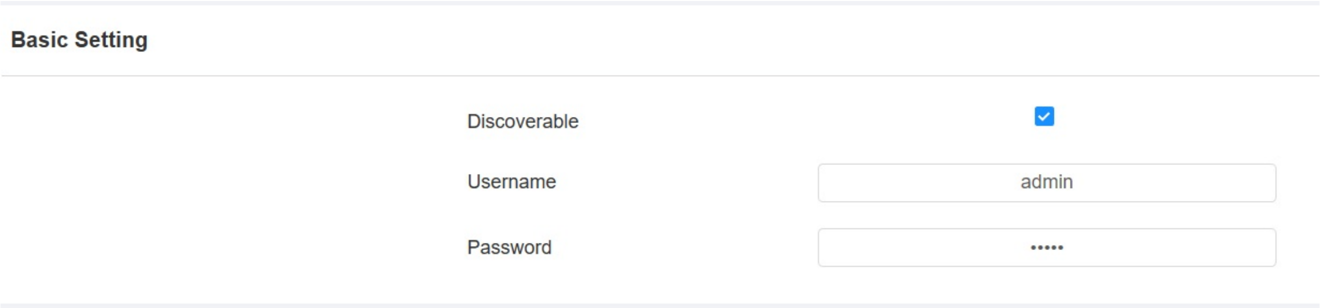
Note

- E18 series supports two video stream channels for H.264 codec video stream.

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.

Path: **Surveillance > ONVIF > Basic Setting**



Basic Setting

Discoverable	☑
Username	admin
Password	•••••

Parameter Set-up:

- **Discoverable**: tick the check box to turn on the ONVIF mode. If you select a video from the door phone camera can be searched by other devices. ONVIF mode is **Discoverable** by default.
- **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

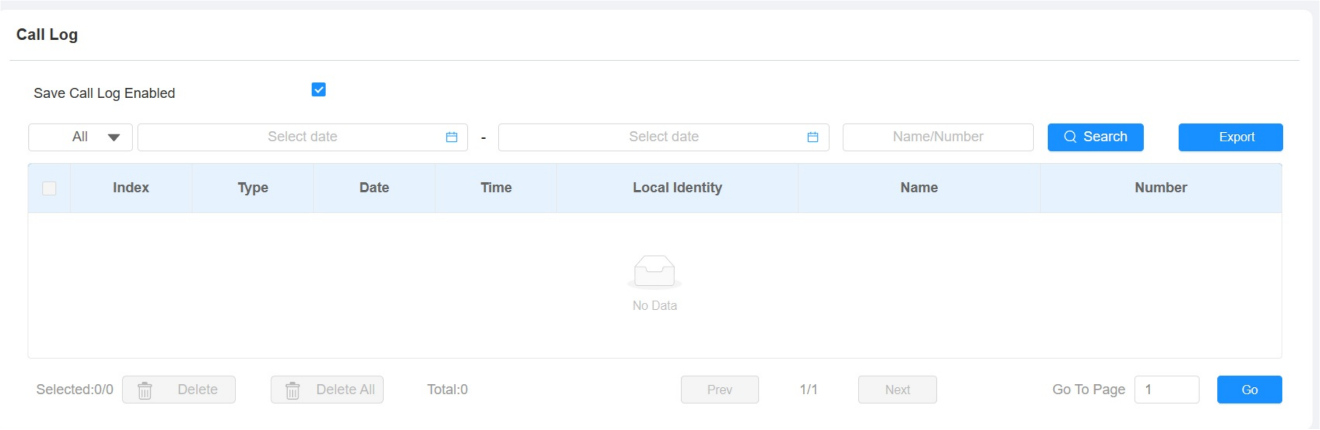
- Fill in the specific IP address of the door phone in the URL.

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.

Path: **Status > Call Log**



Call Log

Save Call Log Enabled ☑

□	Index	Type	Date	Time	Local Identity	Name	Number

No Data

Selected:0/0 Total:0 1/1 Go To Page 1

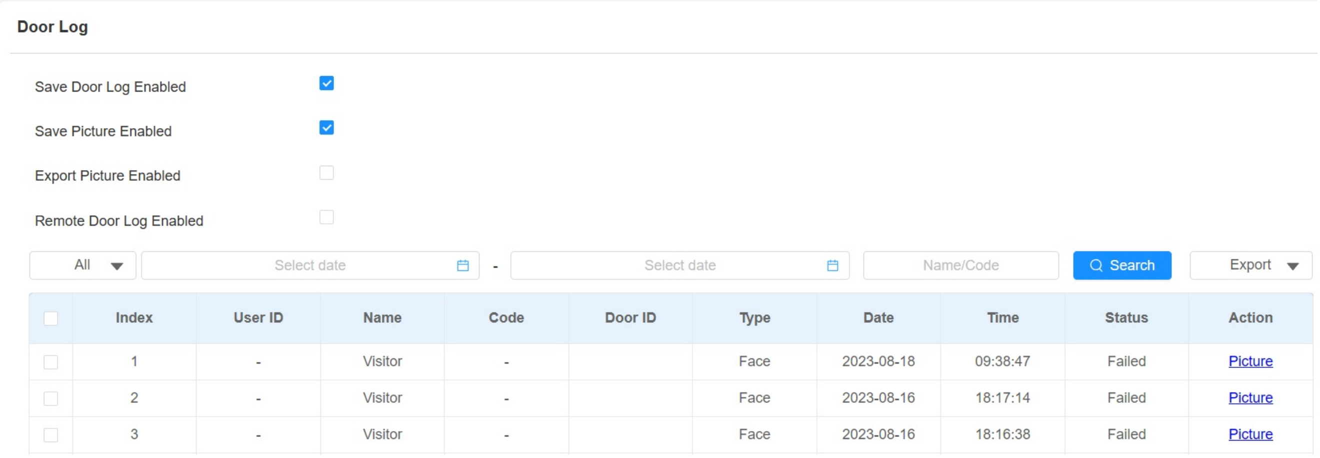
Parameter Set-up:

- **Call History**: select call history among four options: **All, Dialed, Received, Missed** for the specific type of call log to be displayed.

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.

Path: **Status > Access Log**.



Door Log

Save Door Log Enabled ☑

Save Picture Enabled ☑

Export Picture Enabled □

Remote Door Log Enabled □

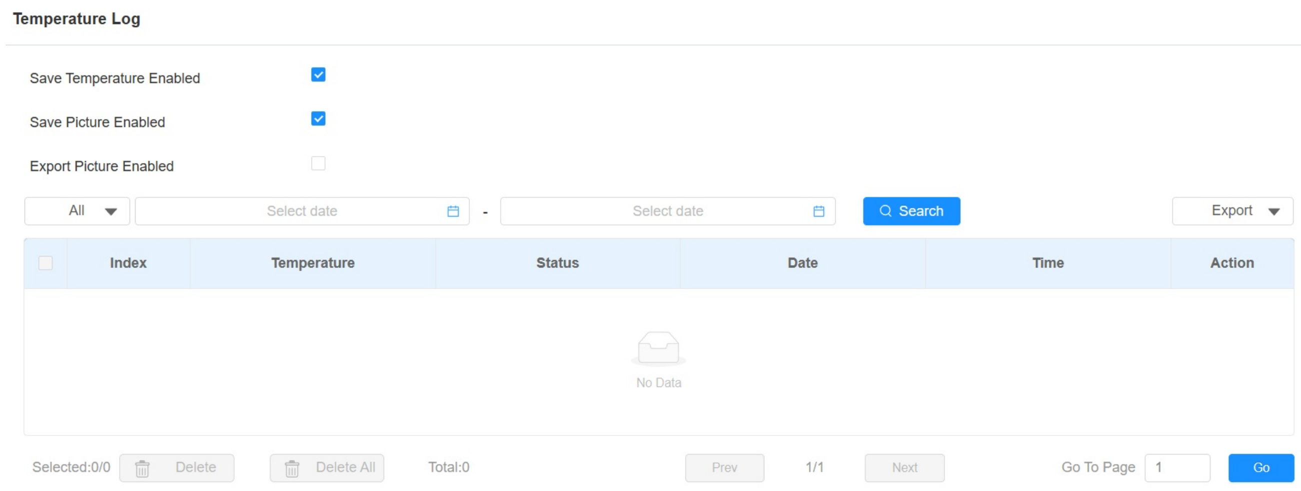
□	Index	User ID	Name	Code	Door ID	Type	Date	Time	Status	Action
□	1	-	Visitor	-		Face	2023-08-18	09:38:47	Failed	Picture
□	2	-	Visitor	-		Face	2023-08-16	18:17:14	Failed	Picture
□	3	-	Visitor	-		Face	2023-08-16	18:16:38	Failed	Picture

Parameter Set-up:

- **Save Picture Enabled**: enable it if you want to save the door open snapshot captured.
- **Export Picture Enabled**: enable it if you want to export the door log with a snapshot picture captured.
- **Status**: select between **Success** and **Failed** options to search for successful door accesses or failed door accesses.
- **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.
- **Action**: click to display the picture captured.

Temperature Log

If you want to search and check on the temperature log, you can search and check the logs on the device web interface. Path: **Status > Temperature Log**



Temperature Log

Save Temperature Enabled ☑

Save Picture Enabled ☑

Export Picture Enabled □

□	Index	Temperature	Status	Date	Time	Action

No Data

Selected:0/0

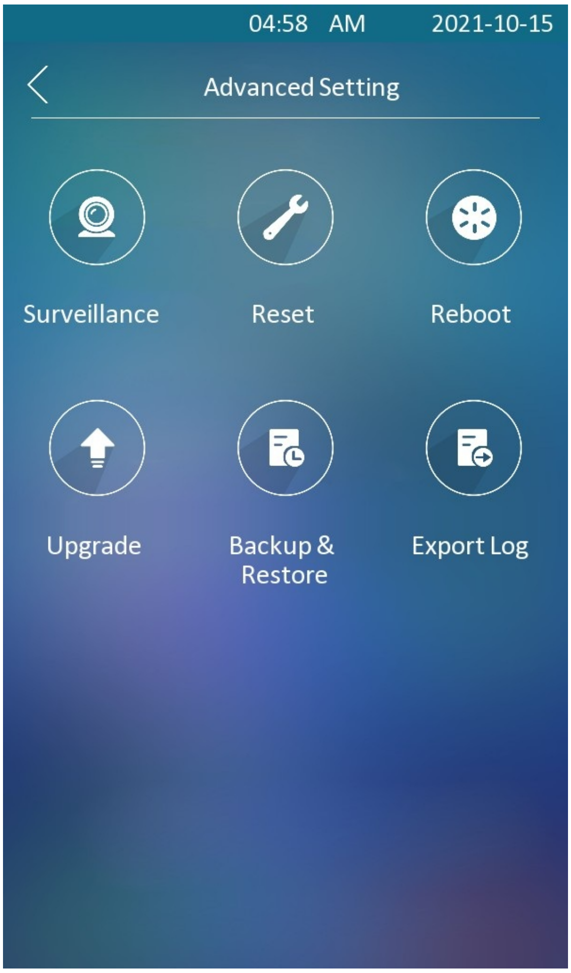
Total:0

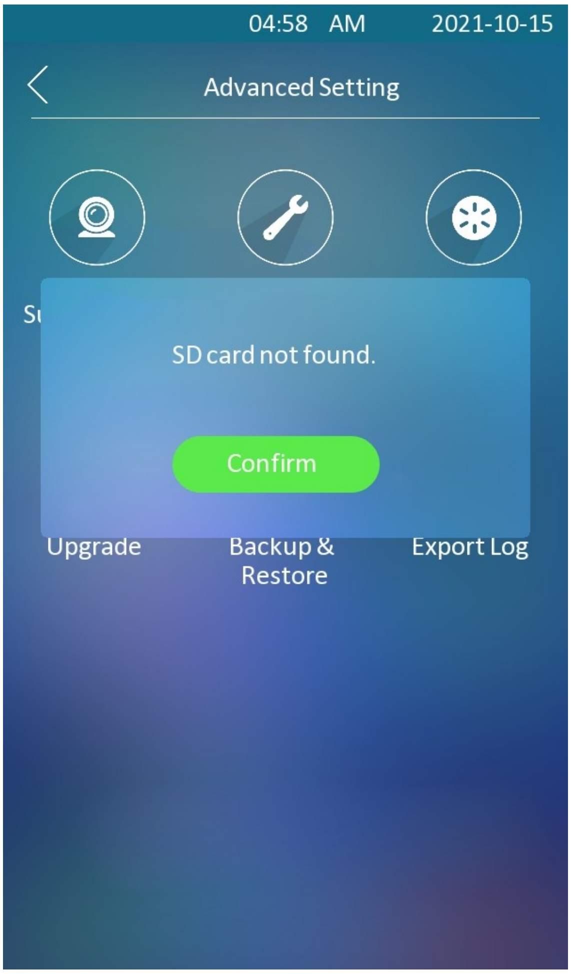
Parameter Set-up:

- **Save Picture Enabled**: enable it if you want to save the temperature-measuring snapshot.
- **Export Picture Enabled**: enable it if you want to export the temperature log with a snapshot picture captured.
- **Time**: select the specific time span of the temperature log you want to search, check, or export.
- **Action**: click to display the picture captured.

Export Logs

You can export door logs, call logs and temperature logs if needed. Path: **Advanced > Export Log.**





SD card not found.

Note

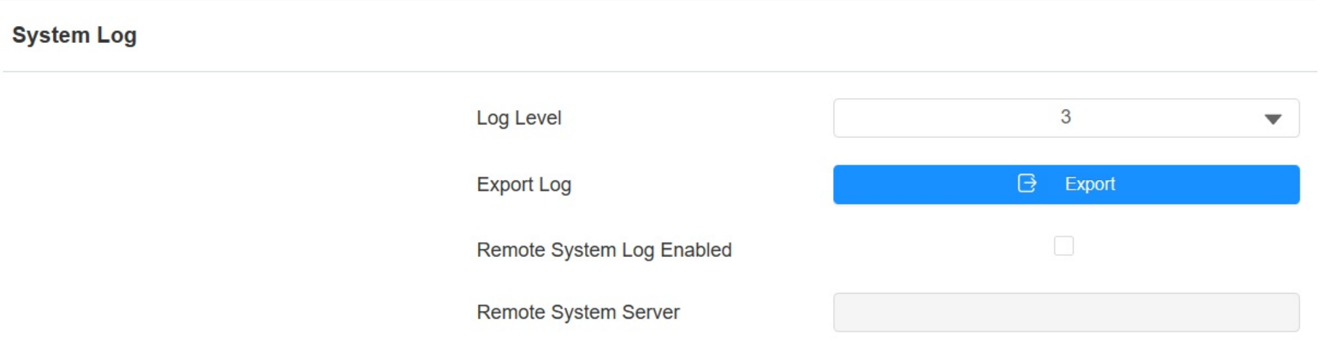
- You need to insert a SD card to export logs on the device screen.

Debug

System Log for Debugging

System logs can be used for debugging purposes.

Path: **System >Maintenance > System Log**



System Log

Log Level	3 ▼
Export Log	Export
Remote System Log Enabled	□
Remote System Server	

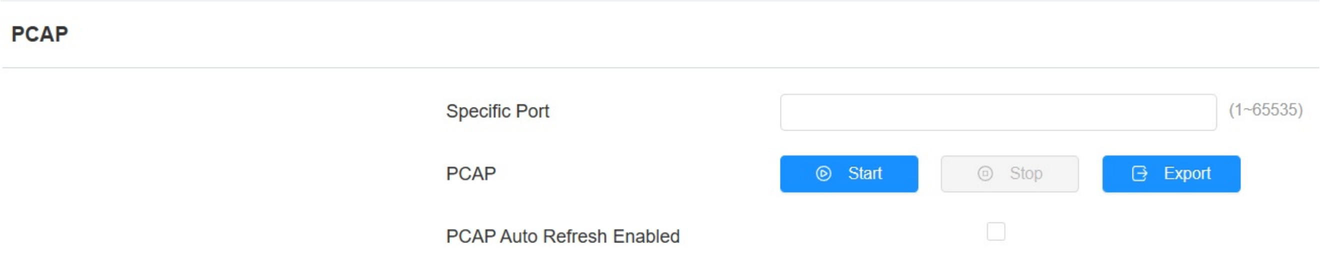
Parameter Set-up:

- **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 **5**, the more complete the log is **7**.
- **Export Log**: click the **Export** tab to export temporary debug log file to a local PC.
- **Remote System Server**: enter the remote server address to receive the device log. 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.

Path: **System >Maintenance > PCAP.**



PCAP

Specific Port	(1~65535)
PCAP	Start Stop Export
PCAP Auto Refresh Enabled	□

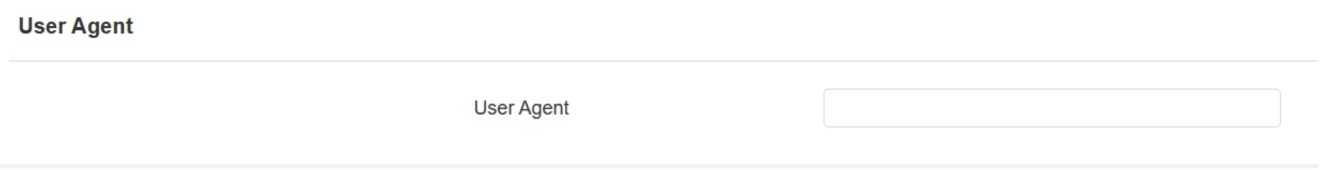
Parameter Set-up:

- **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 **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**: select **Enable** or **Disable** to turn on or turn off the PCAP auto fresh function. If you set it as Enable then the PCAP will continue to capture data packets even after the data packets reached their 1M maximum in capacity. If you set it as Disable the PCAP will stop data packet capturing when the data packet captured reached the maximum capturing capacity of 1MB.

User Agent

User agent is used for identification purpose when you are analyzing the SIP data packet.

Path: **Account > Advanced > User Agent**



User Agent

User Agent

Parameter Set-up:

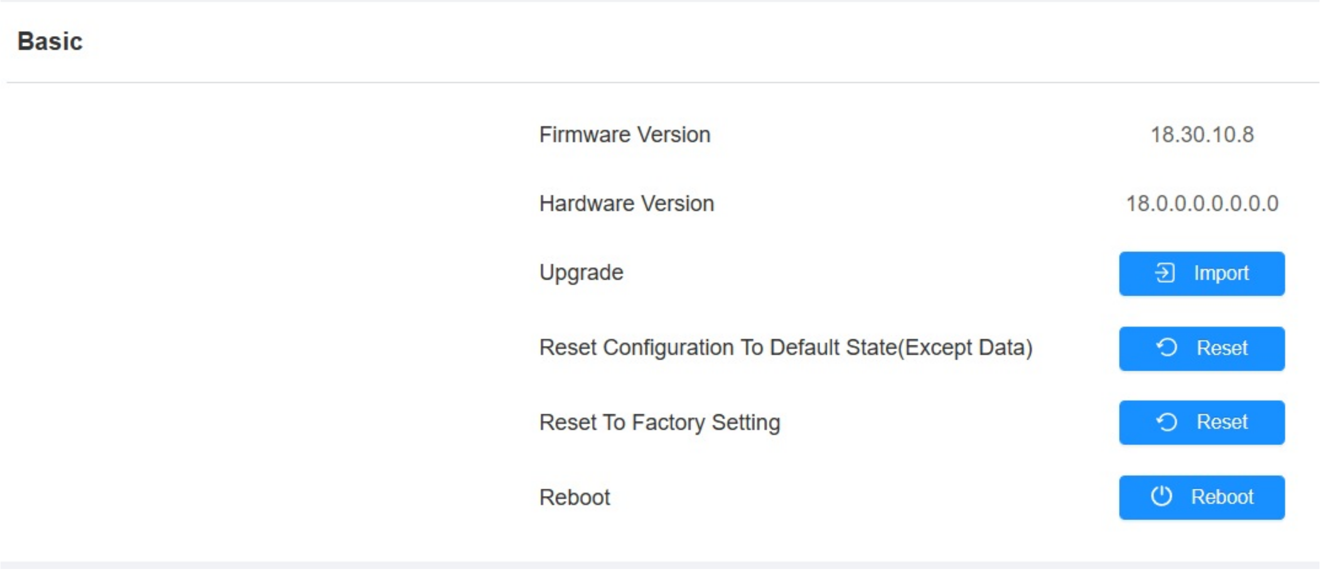
- **User Agent**: support to enter another specific value, it is Akuvox by default.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

- **Upgrade the device on the web interface**

Path: **System > Upgrade.**



Basic

Firmware Version 18.30.10.8

Hardware Version 18.0.0.0.0.0.0.0

Upgrade

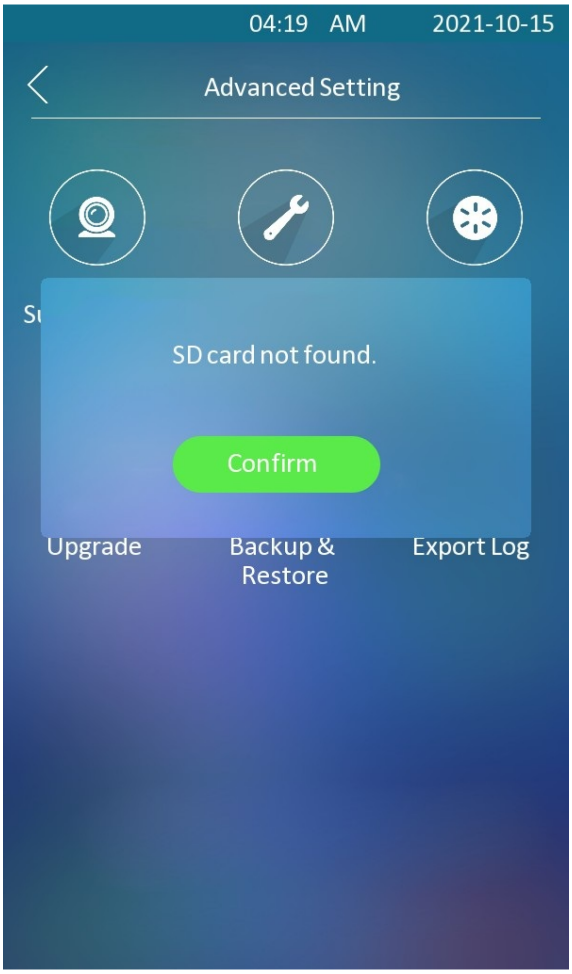
Reset Configuration To Default State(Except Data)

Reset To Factory Setting

Reboot

- **Upgrade the device on the device**

  Path: **Advanced > Upgrade.**



SD card not found.

Note

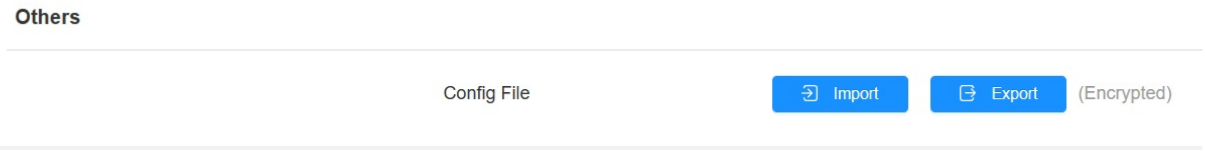
- When you insert the SD card, you are required to add a .rom file at the root directory and change the file name to update.rom.

Backup

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

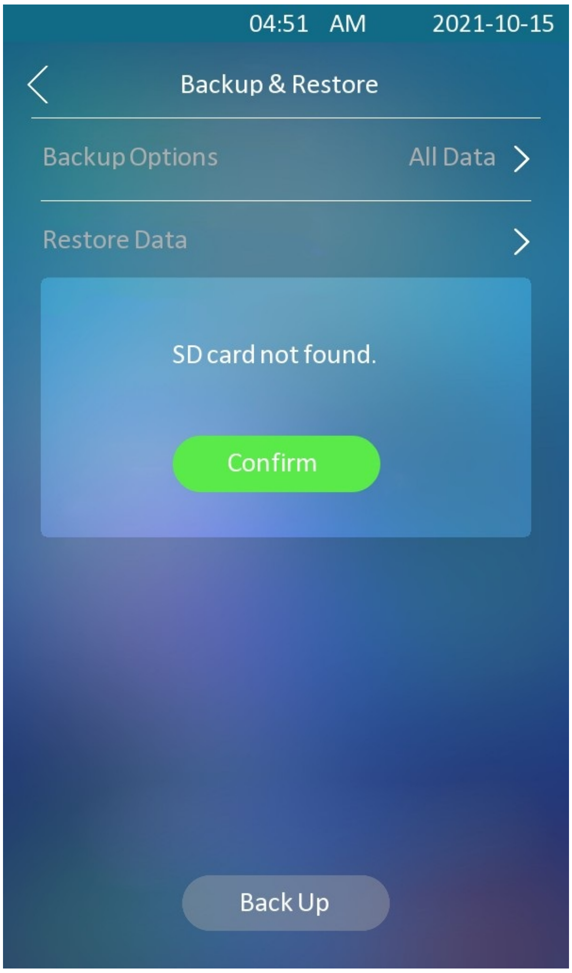
- **Back up data on the web interface**

  Path: **System > Maintenance > Others**



- **Back up data on the device**

  You need to insert the SD card to the device for the backup. Path: **Advanced > Backup&Restore**



Backup Options: All Data

SD card not found.

Parameter Set-up:

- **Backup Options**: select **Only User Data** or **All Data** which is the default setting. Select **All Data** when you want to back up user, group schedule data, and configuration data exclusive of all types of logs. Select **Only User Data** if you only want to back up user and schedule data.

Note

- SDHC and SDXC SD cards with FAT32 format are supported.

Auto-provisioning

Configurations and upgrading on the device can be done 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 access control terminal.

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

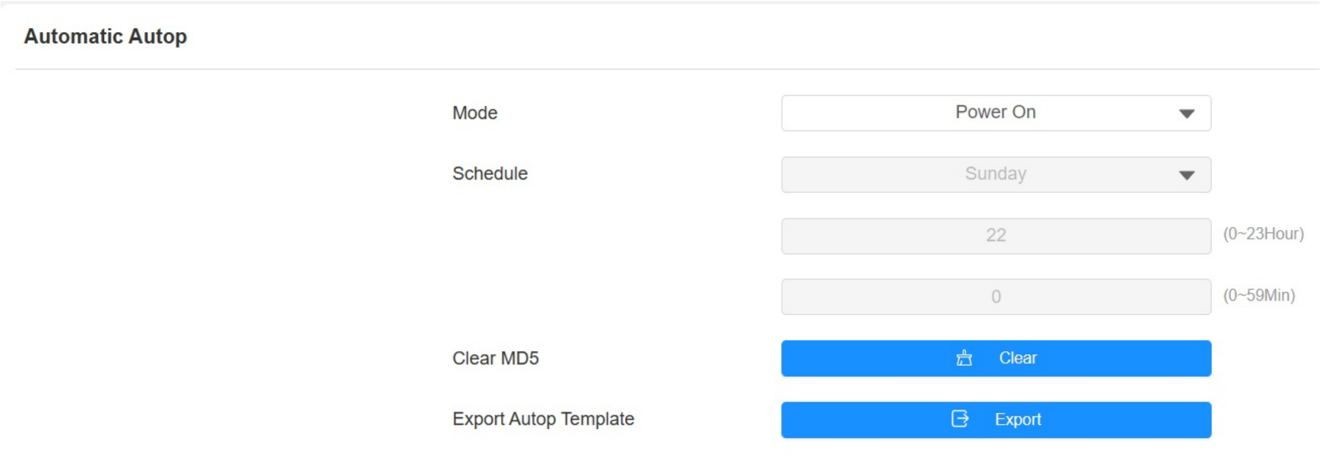
- The configuration file should be in CFG format.
- The general configuration file for the in-batch provisioning varies by model.
- The MAC-based configuration file for the specific device provisioning is named by its MAC address.
- If a server has these two types of configuration files, devices will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

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

AutoP Schedule

Akuvox provides you with different Autop methods that enable the device to perform provisioning for itself according to the schedule.

Path: **System > Auto Provisioning > Automatic Autop**



Automatic Autop

Mode: Power On

Schedule: Sunday

22 (0~23Hour)

0 (0~59Min)

Clear MD5: Clear

Export Autop Template: Export

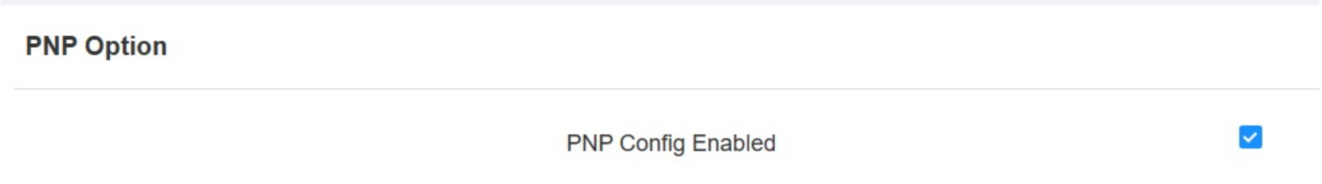
Parameter Set-up:

- **Mode:**
  - **Power On**: select **Power on**, if you want the device to perform Autop every time it boots up.
  - **Repeatedly**: select **Repeatedly**, if you want the device to perform Autop according to the schedule you set up.
  - **Power On + Repeatedly**: select **Power On + Repeatedly** if you want to combine **Power On** Mode and **Repeatedly** mode that will enable the device to perform Autop every time it boots up or according to the schedule you set up.
  - **Hourly Repeat**: select **Hourly Repeat** if you want the device to perform Autop every hour.

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.

Path:**System > Auto Provisioning > PNP Option**

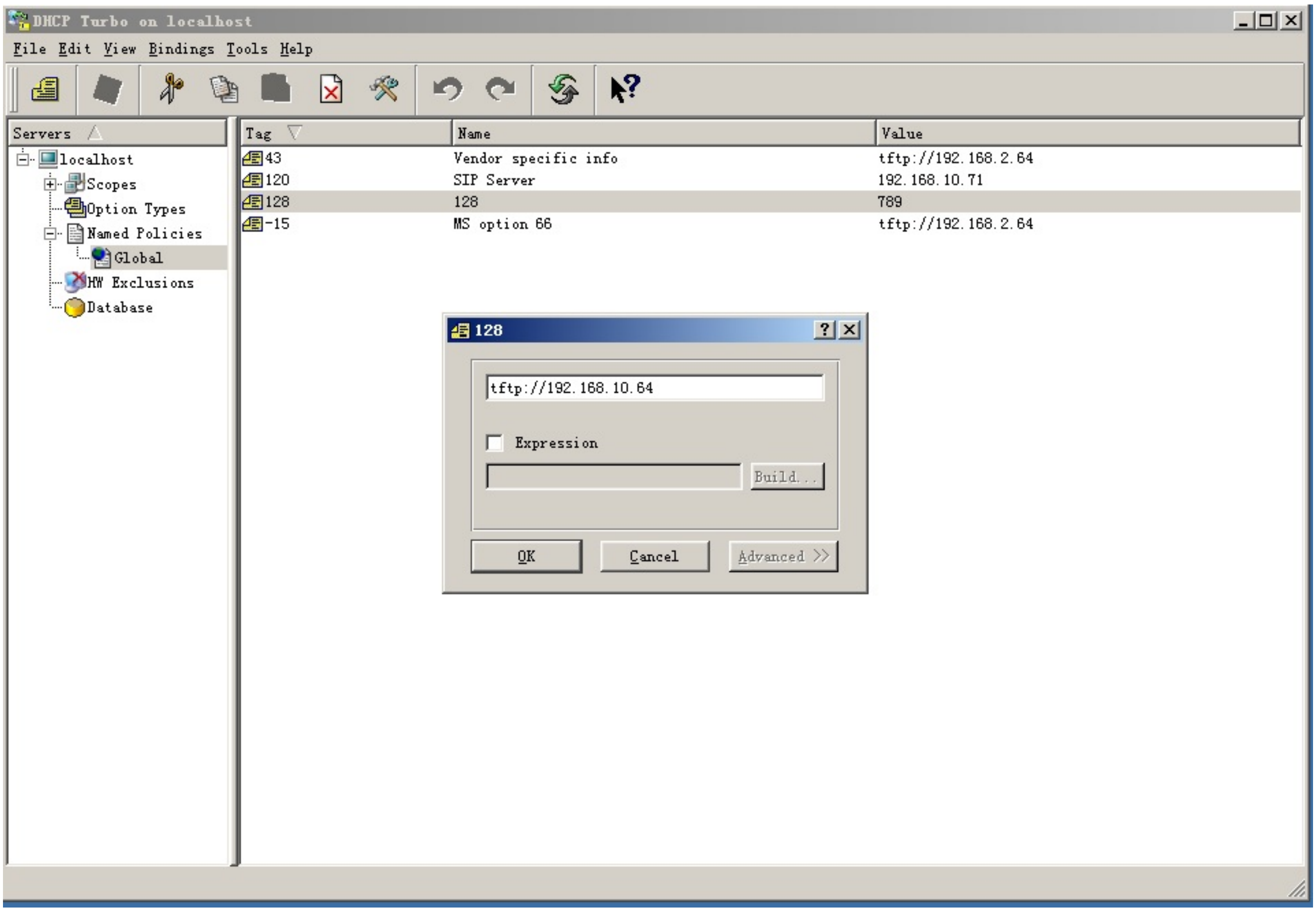


PNP Option

PNP Config Enabled ☑

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.



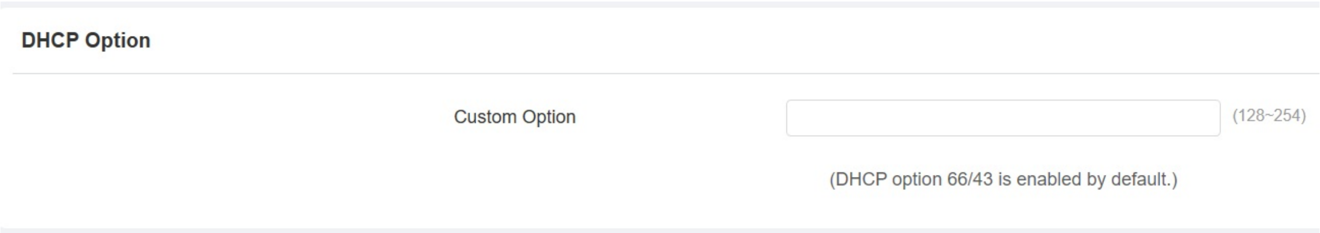
Tag	Name	Value
43	Vendor specific info	tftp://192.168.2.64
120	SIP Server	192.168.10.71
128	128	789
-15	MS option 66	tftp://192.168.2.64

tftp://192.168.10.64

Note

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

Path: **System > Auto Provisioning > DHCP Option.**



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 with corresponding URL so that device will find the configuration file server for the configuration or upgrading.

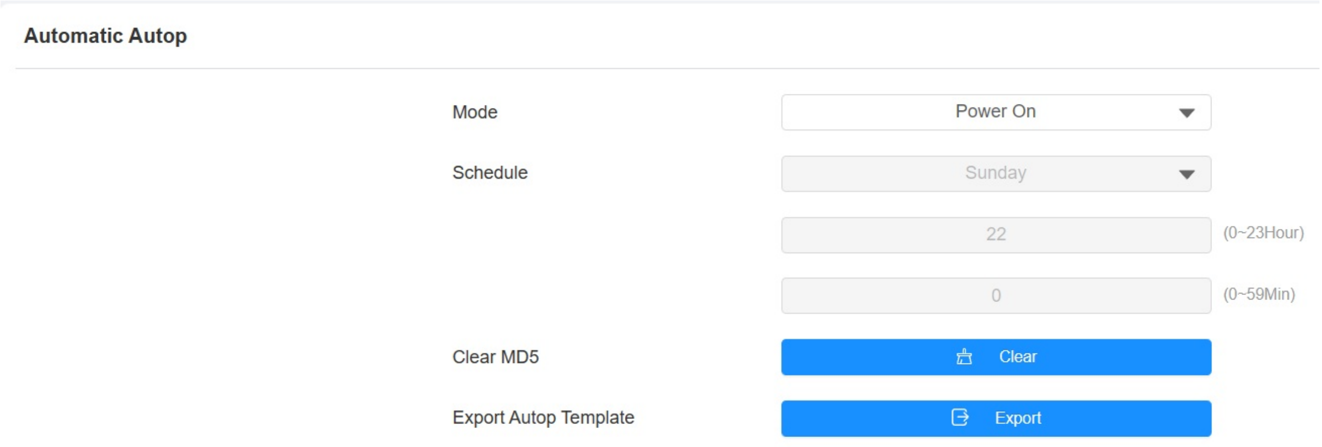
- **DHCP Option 66**: if none of the above is set, the device will automatically use DHCP Option 66 for getting the upgrade server URL. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for the option 66 with the update 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 the option 43 with the update server URL in it.

> **Note**
>
> - The general configuration file for the in-batch provisioning is with the format “cfg”. And taking E18 as an example, “r000000000018.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”.

Static Provisioning Configuration

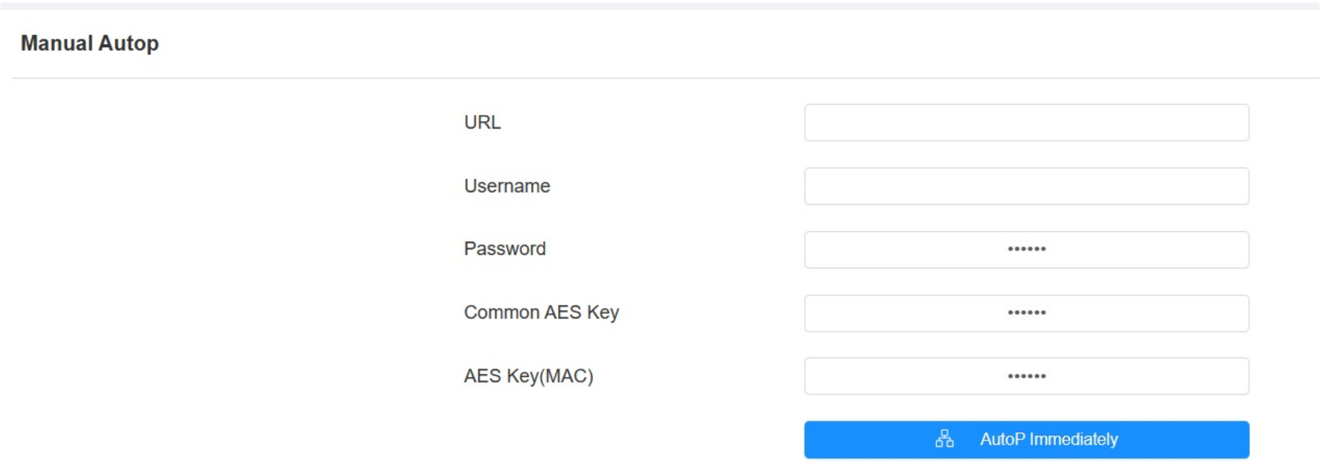
You can manually set up a specific server URL for downloading the firmware or configuration file. If an auto-provision schedule is set up, the device will perform the auto-provisioning at a specific time according to the auto provision schedule you set up. In addition, TFTP, FTP, HTTP, and HTTPS are 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 setup Autop 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 address for the provisioning.
- **User Name**: set up a user name if the server needs an user name to be accessed to otherwise leave it blank.
- **Password**: set up a password if the server needs a password to be accessed to otherwise leave it blank.
- **Common AES Key**: set up AES code for the intercom to decipher general Auto Provisioning configuration file.
- **AES Key (MAC)**: set up AES code for the intercom to decipher the MAC-based Auto Provisioning configuration file.

Tip

- AES, as one type of encryption, should be configured only when the config file is encrypted with AES.

Note

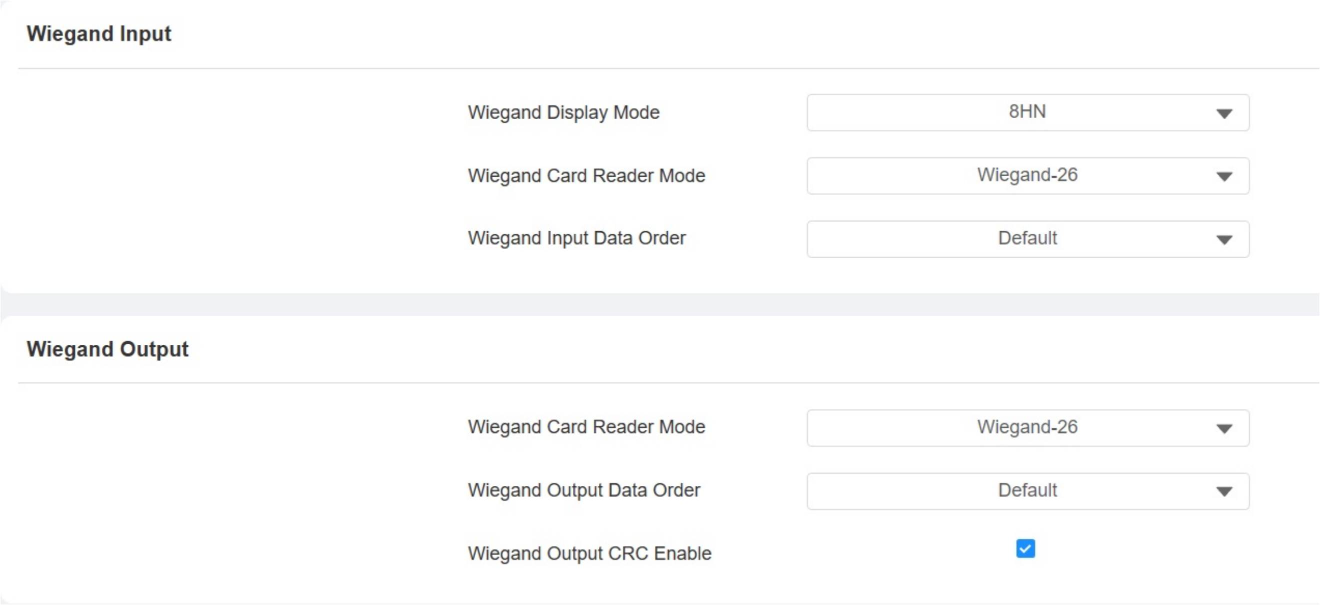
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/ (allows anonymous login)
    ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/ (use the default port 80)
    http://192.168.0.19:8080/ (use other ports, such as 8080)
  - HTTPS: https://192.168.0.19/ (use the default port 443)
- Akuvox does not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

Integration with Third Party Device

Integration via Wiegand

If you want to integrate the door phone with third-party devices via Wiegand, you can configure the Wiegand on the web interface.

Path: **Device > Wiegand**



Wiegand Input

Wiegand Display Mode: 8HN

Wiegand Card Reader Mode: Wiegand-26

Wiegand Input Data Order: Default

Wiegand Output

Wiegand Card Reader Mode: Wiegand-26

Wiegand Output Data Order: Default

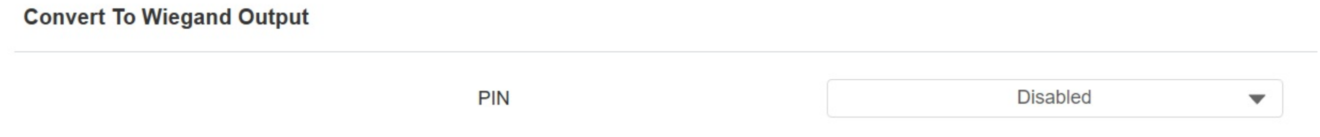
Wiegand Output CRC Enable: ☑

Parameter Set-up:

- **Wiegand Display Mode**: select Wigand Card code format among **8H10D; 6H3D5D; 6H8D; 8HN; 8HR; RAW; 8HR10D**.
- **Wiegand Card Reader Mode**: set the Wiegand data transmission format among three options: **Wiegand 26, Wiegand 34**, and **Wiegand 58**. The transmission format should be identical between the door phone and the device to be integrated.
- **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 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**: tick to enable the parity check function to ensure that signal-based data can be transmitted correctly according to the established data transmission

format.

When integrating with third-party devices, you need to set up the Wiegand PIN code output based on the Wiegand output format of the third-party device.



Convert To Wiegand Output

PIN: Disabled

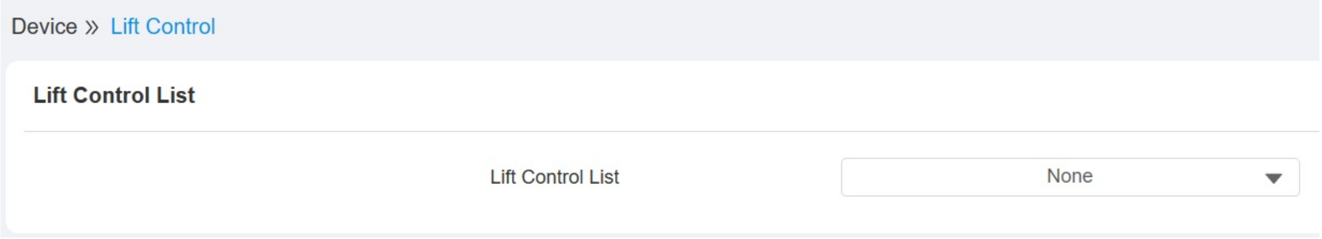
Parameter Set-up:

- **8 bits per digit**: select it if the third-party device adopts **8 bits per digit** format. The PIN code is transferred separately by a digit (one digit consists of 8 bits).
- **4 bits per digit**: select it if the third-party device adopts **4 bits per digit** format. The PIN code is transferred separately by a digit (one digit consists of 4 bits).
- **All at once**: select it if the third-party device adopts **All at once** format. When it is selected, the PIN code will not be transferred until you enter the whole PIN code.

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, go to **Device > Lift Control**.



Device » Lift Control

Lift Control List

Lift Control List: None

Parameter Set-up:

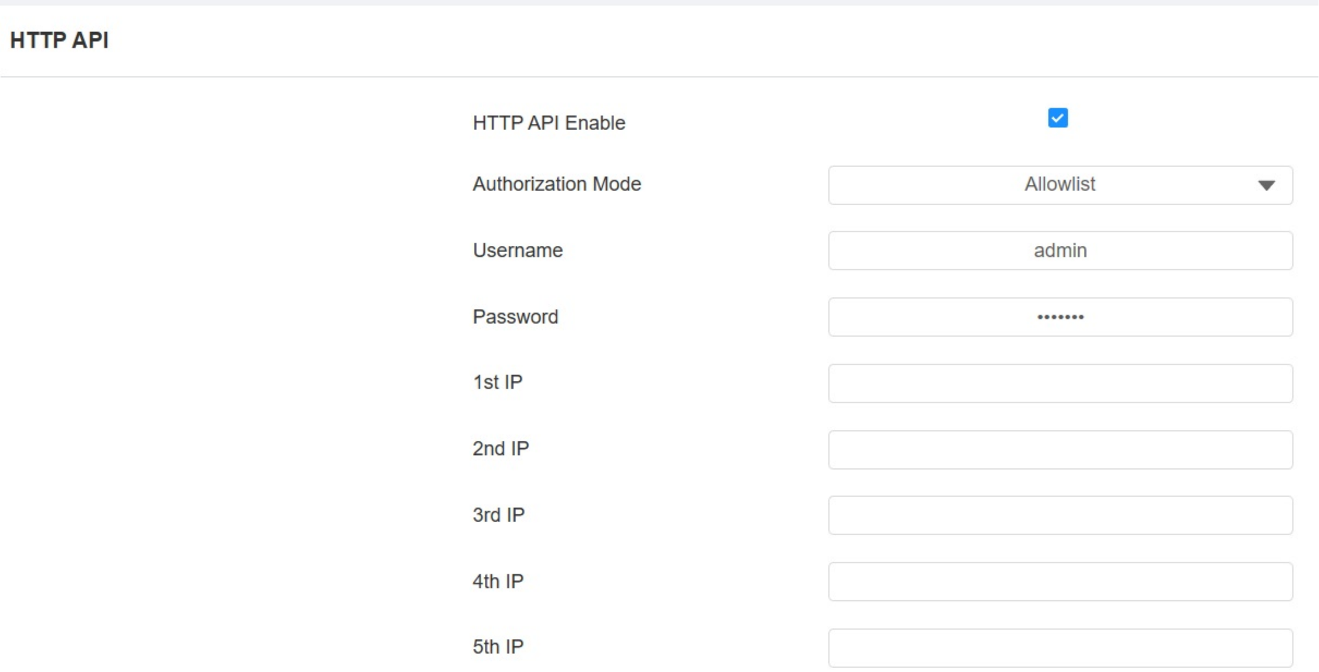
- **Lift Control List**: select integration mode among **None, OSDP, Akuvox EC32, KEYKING.** The detail for the options will be provided in the following chart.

No.	Integration Mode	Description
1	None	If you select **None**, then the RS485 integration will be disabled.
2	OSDP	If you select **OSDP** Mode, then the integration communication between the door phone and the third-party device is via OSDP protocol. You are required to check for the device integration protocol and make sure that they use the same integration protocol.
3	Akuvox EC32	Select **Akuvox EC32** if you want to connect the device with the Akuvox EC32 lift controller.
4	KEYKING	Select **KEYKING** if you want to integrate with the KEYKING lift controller.

Integration via HTTP API

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

Path: **Setting > HTTP API**



HTTP API

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

Parameter Set-up:

- **HTTP API Enable**: enable or disable the HTTP 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 to HTTP 403 forbidden status.
- **Authorization Mode**: select among four options: **None, Allowlist, Basic, Digest**, and **Token** for authorization type, which will be explained in detail in the following chart.
- **Username**: 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 user name is admin.
- **1st IP- 5th IP**: enter the IP address of the third-party devices when the WhiteList authorization is selected for the integration.

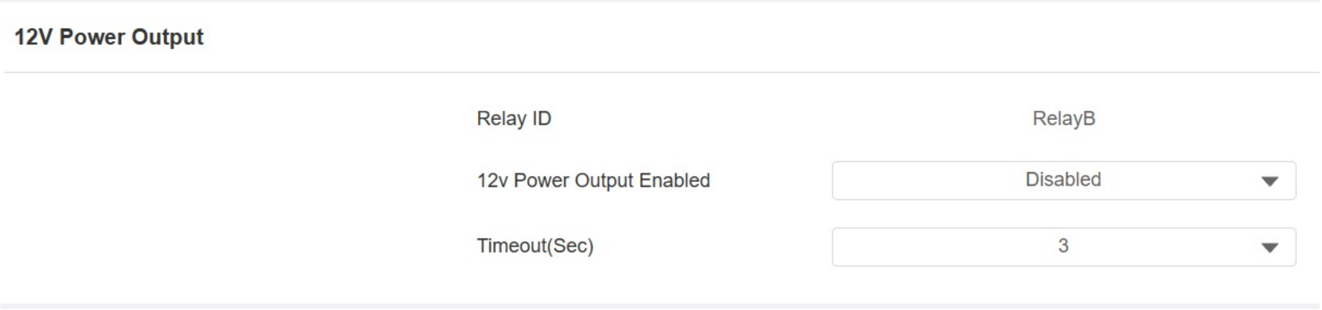
Please refer to the following description for the Authentication mode:

NO.	Authorization Mode	Description
1	None	No authentication is required for HTTP API as it is only used for demo testing.
2	Allow List	If this mode is selected, you are only required to fill in the IP address of the third party device for the authentication. The whitelist is suitable for operation in the LAN.
3	Basic	If this mode is selected, you are required to fill in the User name and the password for the authentication.In Authorization field of HTTP request header, use Base64 encode method to encode of username and password.
4	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".
5	Token	This mode is used by Akuvox developer only.

Power Output Control

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

Path: **Access Control > Relay >12V Power Output**



12V Power Output

Relay ID: RelayB

12v Power Output Enabled: Disabled

Timeout(Sec): 3

Parameter Set-up:

- **Relay ID**: select the relay to be powered by E18.
- **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 E18 to provide power to the third party device via 12 output and GND interface during the timeout when the relays status is shifted from low to high.
- **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.

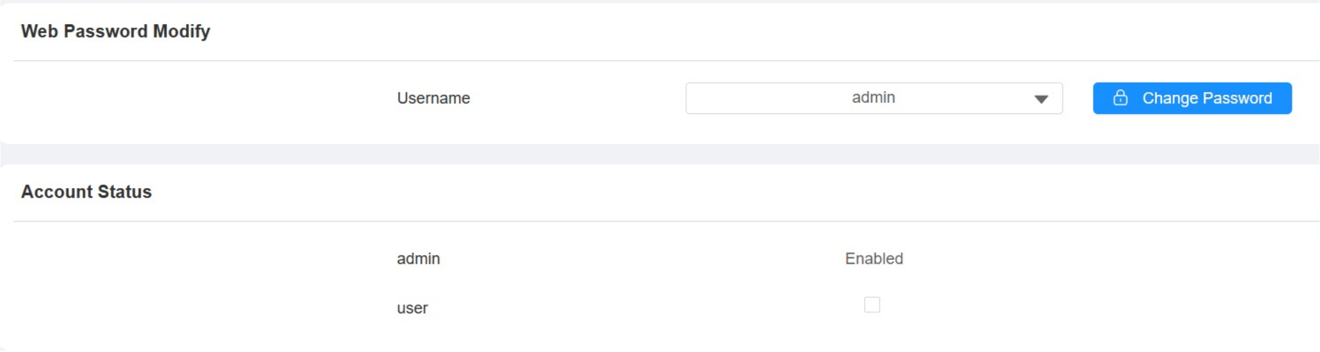
Password Modification

On the device web interface, you can set and change both the System PIN Code for accessing the device setting and login password for accessing the web interface. In addition, you can also select the user role when setting passwords.

Modify Device Web Interface Password

To modify web interface password, you can do it on device web interface. Select **Admin** for the administrator account and **User** for the User Account. Click the **Change Password** tab to change the password.

Path: **System** > **Security** > **Web Password Modify**

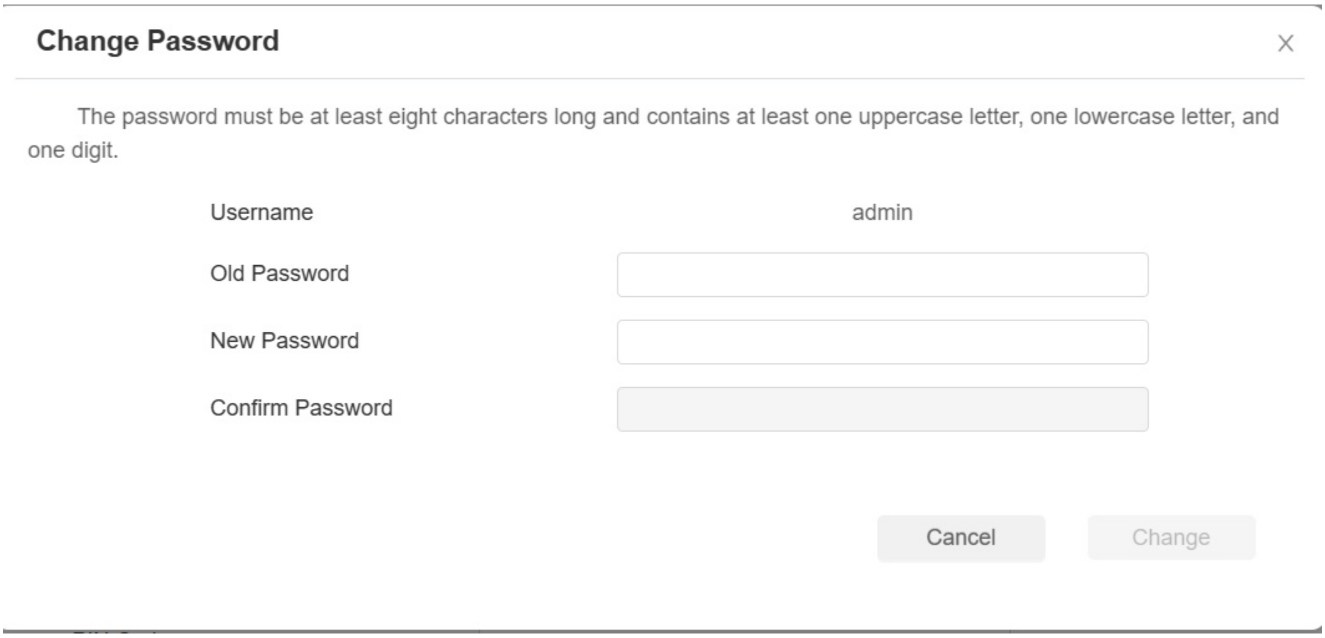


Web Password Modify

Username: admin ▾ | Change Password

Account Status

admin	Enabled
user	☐



Change Password ×

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

Username: admin

Old Password:

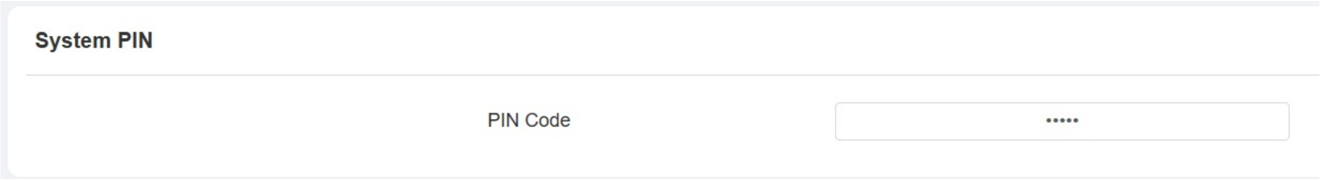
New Password:

Confirm Password:

Cancel | Change

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.



System PIN

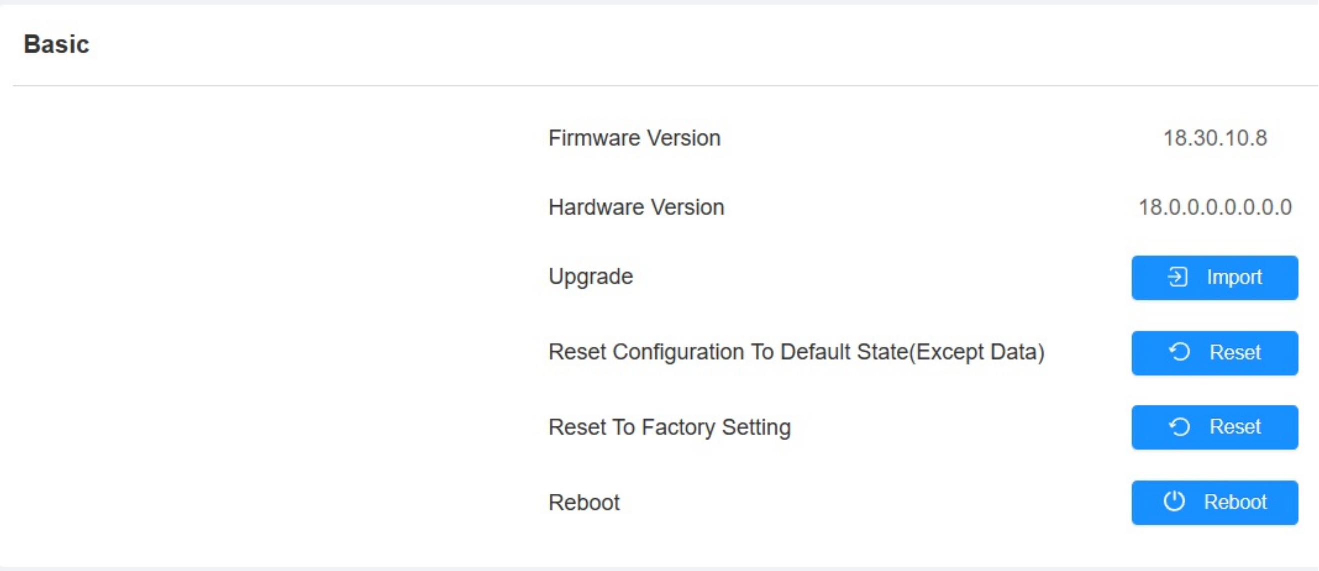
PIN Code •••••

System Reboot&Reset

Reboot

If you want to restart the device system, you can operate it on the device web interface as well. Moreover, you can set up a schedule for the device to be restarted.

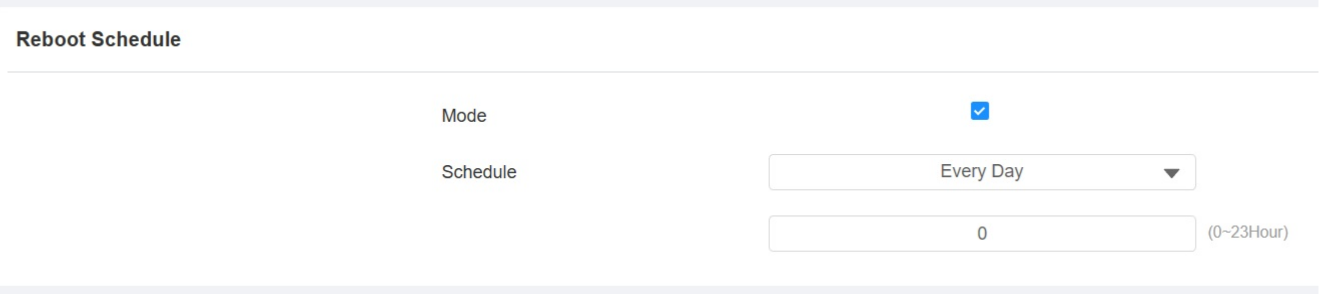
To reboot the system setting on the web **System > Upgrade** interface.



Basic

Firmware Version	18.30.10.8
Hardware Version	18.0.0.0.0.0.0
Upgrade	Import
Reset Configuration To Default State(Except Data)	Reset
Reset To Factory Setting	Reset
Reboot	Reboot

To set up the device reboot schedule, go to **System > Auto Provisioning > Reboot Schedule.**



Reboot Schedule

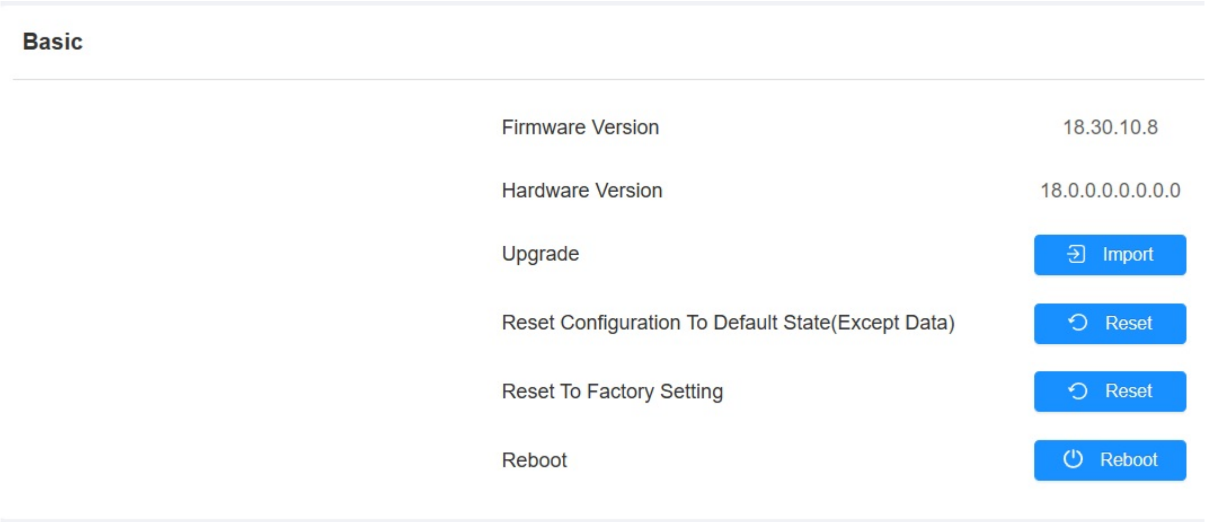
Mode	☑
Schedule	Every Day
	0 (0~23Hour)

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).

Path: **System > Upgrade > Basic**

- **To reset the device on the device web interface**

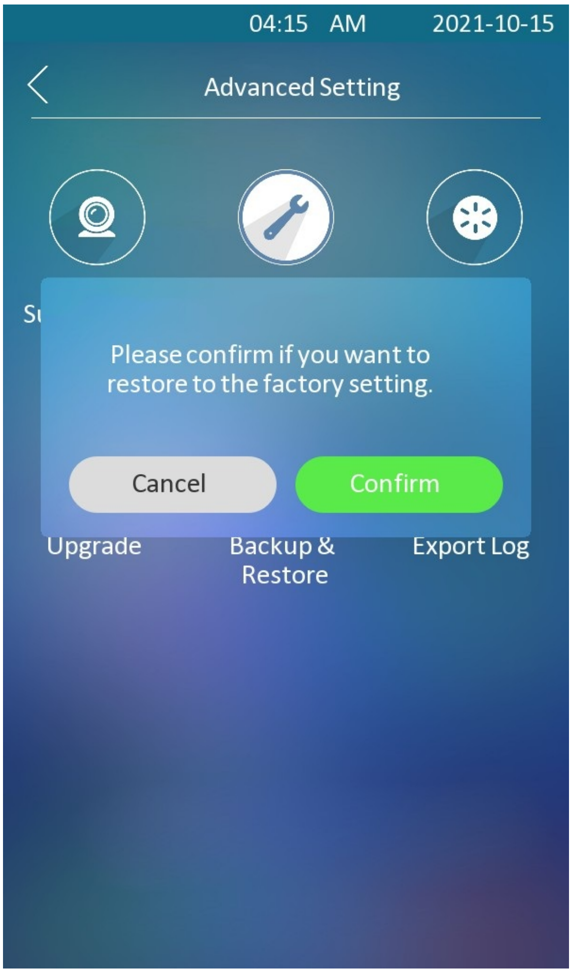


Basic

Firmware Version	18.30.10.8
Hardware Version	18.0.0.0.0.0.0.0
Upgrade	Import
Reset Configuration To Default State(Except Data)	Reset
Reset To Factory Setting	Reset
Reboot	Reboot

- **To reset the device on the device**

  Path: **Advanced > Reset**



04:15 AM 2021-10-15

Advanced Setting

Please confirm if you want to restore to the factory setting.