Akuvox
Open A Smart World

WWW.AKUVOX.COM

E16 SERIES DOOR PHONE

Administrator Guide

About This Manual

Thank you for choosing Akuvox E16C door phones. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to the 216.30.0.35 version, and it provides all the configurations for the functions of E16C door phones. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

FCC Caution:

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .

This transmitter must not be co - located or operating in conjunction with any other antenna or transmitter.

This equipment should be installed and operated with minimum distance 20cm between the radiator& your body.

Introduction of Icons and Symbols

Note

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

Related Documentation

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

https://knowledge.akuvox.com

Content

1 Product Overview

Akuvox E16C products are Android-based IP video door phones with touch screens. It incorporates audio and video communications, access control, and video surveillance. Its finely-tuned Android OS, SmartPlus, and AI-based communication technology allow featured customization to better suit your operation habits. E16C multiple ports, such as RS485 and Wiegand ports, can be used to easily integrate external digital systems, such as elevator controllers and fire alarm detectors, helping to create a holistic control of the building entrance and its surroundings and giving you a great sense of security via a variety of access such as card access, NFC, Bluetooth, QR code and newly added door access in an accompaniment with body temperature measurement. E16C door phones apply to residential buildings, office buildings, and their complex.

2 Change Log

The change log will be updated here along with the changes in the new software version.

3 Model Specification

Model & Feature	E16C
Display	5" IPS
Touch Screen	√
Button	X
Housing Material	Plastic
Relay Out	1
Alarm In	1
RS485	√
PoE	√
Resolution	1280x720

Brightness	500cd/m^2
RAM	1GB
ROM	8GB
Card Reader	13.56MHz
Wi-Fi	X
Bluetooth	√
IP Rating	IP65
Temperature Detection	Optional
Face recognition	√
LTE	X
USB	X
External SD Card	X
Wall Mounting	√
Flush Mounting	√
Desk Mounting	X
POE Stand by Power	5.5W

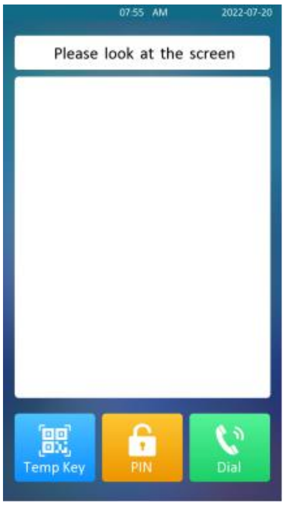
POE Full Load Consumption	9.8W
Power Adapter Standby Power	5.5W
Power Adapter Full Load Consumption	10W
Color Option	Black
Wall Mounting	√
Flush Mounting	√
Desk Mounting	X
POE Stand by Power	5.5W
POE Full Load Consumption	9.8W
Power Adapter Standby Power	5.5W
Power Adapter Full Load Consumption	10W
Color Option	Black

4 Access the Device

E16C door phones' system settings can be either accessed on the device directly or on the device web interface.

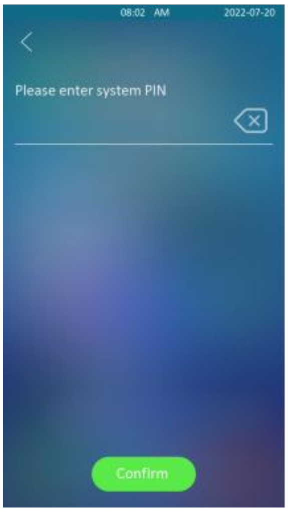
4.1 Access the Device Setting on the device

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



07:55 AM 2022-07-20

Please look at the screen

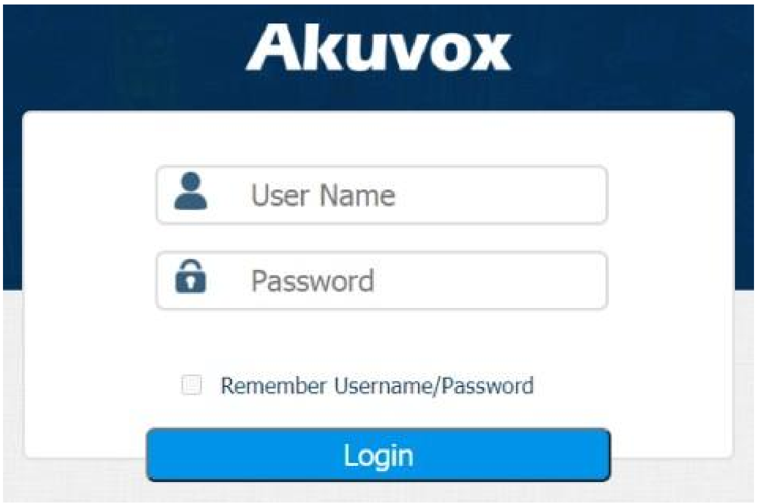


08:02 AM 2022-07-20

Please enter system PIN

4.2 Access the Device Setting on the Web Interface

You can also use the Akuvox IP scanner tool to search the device's IP address on the same LAN. Then enter the device IP address on the web browser in order to login to the device web interface where you can configure and adjust parameters etc. Then use the IP address to login into the web browser by user name and password **admin** and **admin**.



Note

- You can also obtain the device IP address using the Akuvox IP scanner to log into the device web interface. Please refer to the URL below for the IP scanner application:

https://knowledge.akuvox.com/docs/how-to-obtain-ip-address-via-ip-scanner-1

Note

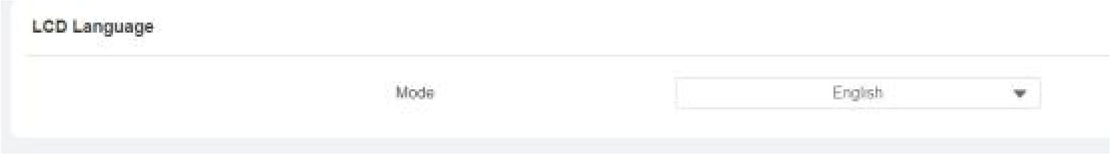
- Google Chrome browser is strongly recommended.
- The initial user name and password are **admin** and please be case-sensitive to the user names and passwords entered.

5 Time and Language Setting

5.1 Language Setting

You can select device language, and customize interface text including configuration names and prompt text display on the device and on the web interface.

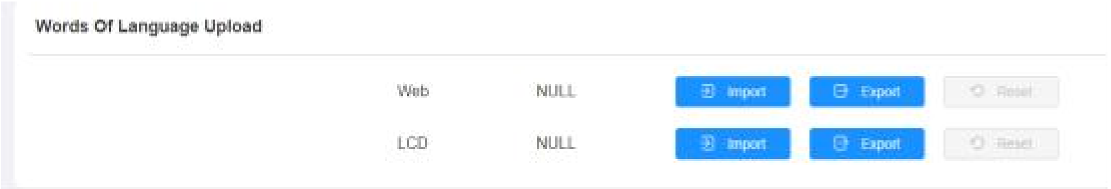
To select the device language, go to **Setting > Time/Lang > LCD Language** interface.



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. **Setting > Time/Lang > Words Of Language Upload.**

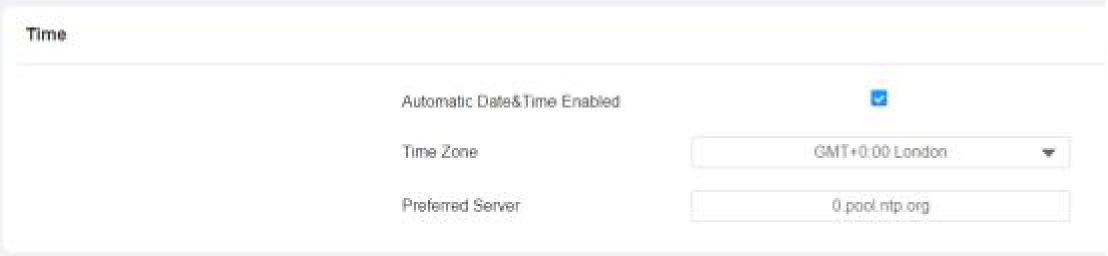


Words Of Language Upload

Web	NULL	Import	Export	Reset
LCD	NULL	Import	Export	Reset

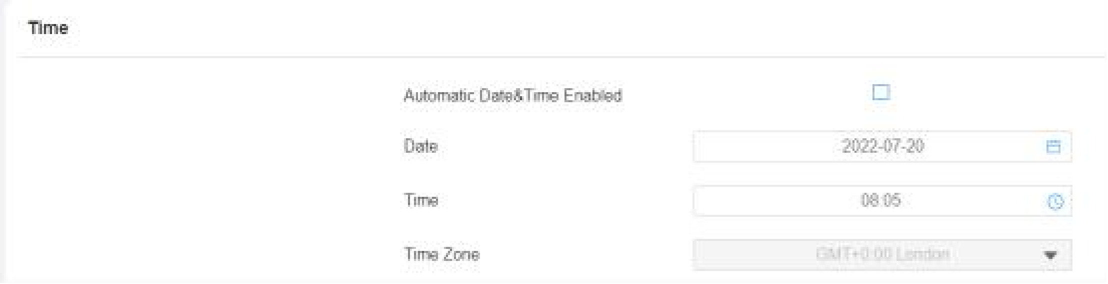
5.2 Time Setting

Time setting on the web **Setting > Time/Lang > Time** interface allows you to set up time and date manually while allowing you to use the NTP server address that you obtained to automatically synchronize your time and date. And when your time zone is selected, the device will automatically notify the NTP server of its time zone so that the NTP server can synchronize the time zone setting in your device.



Time

Automatic Date&Time Enabled	☑
Time Zone	GMT+0:00 London
Preferred Server	0.pool.ntp.org



Time

Automatic Date&Time Enabled	□
Date	2022-07-20
Time	08:05
Time Zone	GMT+0:00 London

Parameter Set-up:

- **Automatic Date&TimeEnabled:** enable it if you want the device's date and time to be automatically set up and synchronized with the default time zone and the NTP server (**Network Time Protocol**).
- **Time Zone:** select the specific time zone depending on where the device is used and then press **Confirm** tab for the confirmation. The default time zone is GMT+0.00.
- **Primary Server**: enter the primary NTP server you obtained in the **NTP Server**.
- **Date/Time**: set the date and time for the device manually when you disable the automatic date and time service.

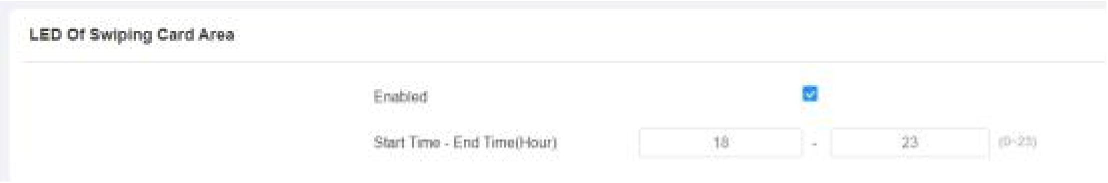
Note

- When the check box is not ticked, parameters related to the NTP server cannot be edited.

5.3 LED Setting

5.3.1 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 the card reader LED light to stay on, you can also set the timing for the exact time span during which the LED light can be disabled to reduce the electrical power consumption. To configure the configuration on the web **Device > Light > LED Of Swiping Card Area** interface.



LED Of Swiping Card Area

Enabled ☑

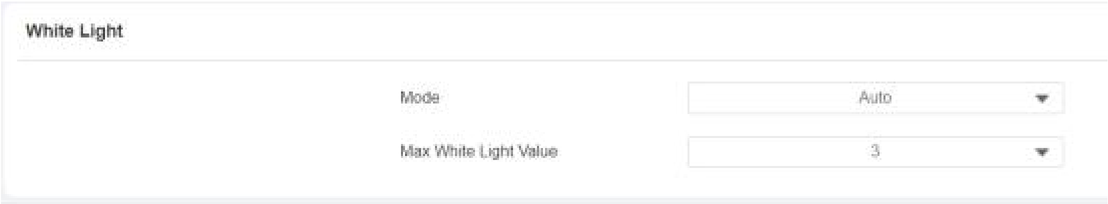
Start Time - End Time(Hour) 18 - 23 (0-23)

Parameter Set-up:

- **Enabled**: tick the check box you want to enable the card reader LED lighting and vice versa.
- **Start Time- End Time (H)**: enter the time span for the LED lighting to be valid, eg. 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).

5.3.2 Configure LED White Light Setting

LED White light is used to reinforce the lighting for facial recognition as well as for QR code access in the dark environment. To configure the function, go to **Device > Light > White Light** interface.



White Light

Mode: Auto

Max White Light Value: 3

Parameter Set-up:

- **Mode**: if you select **Auto**, then the white light will be turned on automatically for face recognition and QR code scan for door opening. If you select **Off**, then the white light will be disabled.
- **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

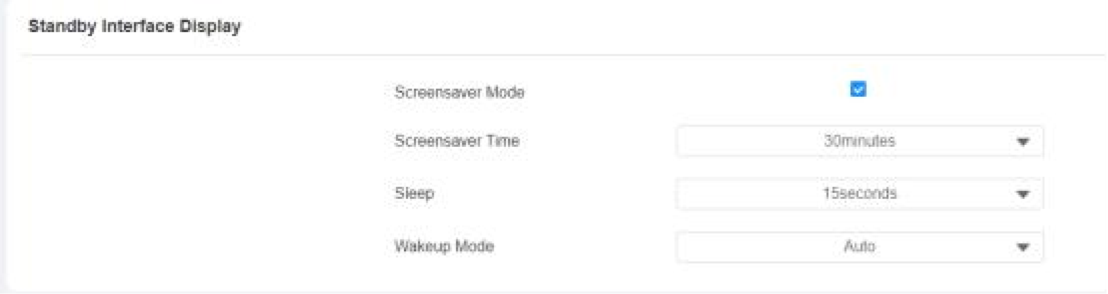
- IR LED light should be triggered first before the white light can be valid in the facial recognition, however, IR LED light does not need to be triggered for the white light function in the QR code scan.

5.4 Screen Display configuration

E16C door phones allow you to enjoy a variety of screen displays to enrich your visual and operational experience through the customized setting to your preference.

5.4.1 Configure Screensaver

Await screen is mainly a function for screen protection. You can make the device go into idle status for a predefined time span when there is no operation on the device, or no one is detected approaching. To configure the configuration on web **Device > LCD > Standby Interface Display** interface.



Standby Interface Display

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

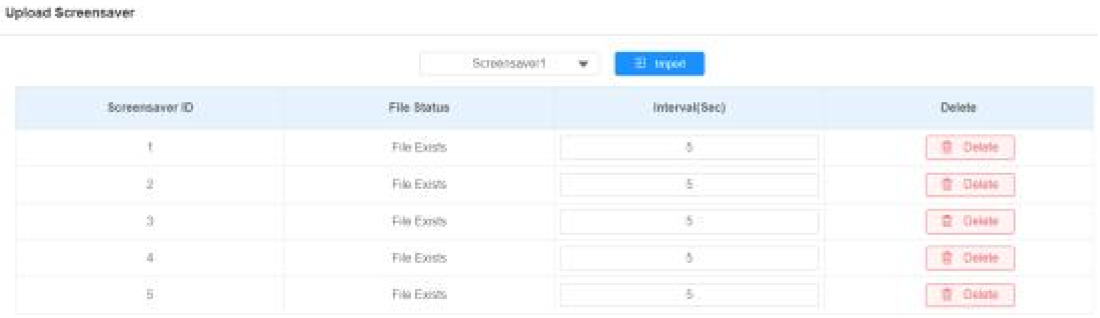
Parameter Set-up:

- **ScreenSaver Mode:** tick the check box to enable the screen saverfunction.

- **Screensaver Time (Sec)**: set the screen saver start time from 5 seconds up to 2. For example, if you set the start time as 5 minutes, then the screen saver will start if there is no operation on the device or no one is approaching during the five minutes interval.
- **Sleep:** set how long you expect the screen saver to last before turning off the device's screen. You select the screen saver duration from 2 seconds to 30.
- **Wakeup Mode**: select the screen wake-up 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.

5.4.2 Upload Screensaver

You can upload screensaver pictures separately or in batch to the device and to the device web interface. To configure the configuration on web **Device > LCD > Upload Screensaver** interface. You can upload a maximum of 5 pictures, and each picture will be displayed in rotation according to the ID order with a specific time duration (**Time Interval**) you set.



Upload Screensaver

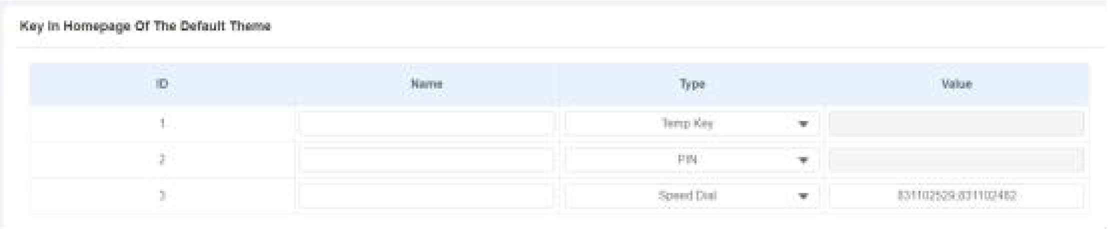
Screensaver ID	File Status	Interval(Sec)	Delete
1	File Exists	5	Delete
2	File Exists	5	Delete
3	File Exists	5	Delete
4	File Exists	5	Delete
5	File Exists	5	Delete

Note

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

5.4.3 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		Speed Dial	831102529;831102482

Parameter Set-up:

- **Name**: enter a new name to replace the original type of name, but it does not change the attribute of the type.
- **Type**: select the tab type corresponding to the index number which indicates the tab position. For example, if you want to make the **Speed Dial** tab 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.
- **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. You can type in five-speed dial numbers maximum and every two of the number must be separated by “;”.

5.5 Volume & Tone Configuration

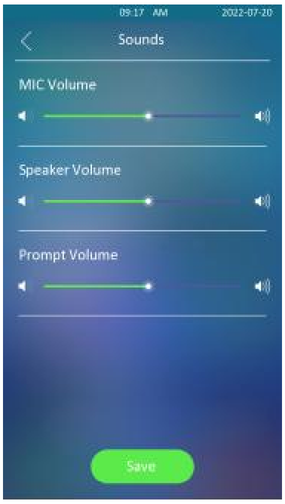
Volume and tone configuration in E16C door phone refers to the call volume (speaker), Mic volume, and prompt volume (eg. open door tone). Moreover, you can upload the tone you like to enrich your personalized user experience.

5.5.1 Volume Configuration

You can configure the Mic volume, speaker volume, and temper alarm volume according to your need for intercom-based audio&video communication. Moreover, you can also set up the tamper alarm volume when unwanted removal of the door phone occurs.

5.5.1.1 Configure Volume on the Device

You can adjust the microphone volume, speaker volume, and prompt volume on the device. Path: **Display&Sounds > Sounds**.

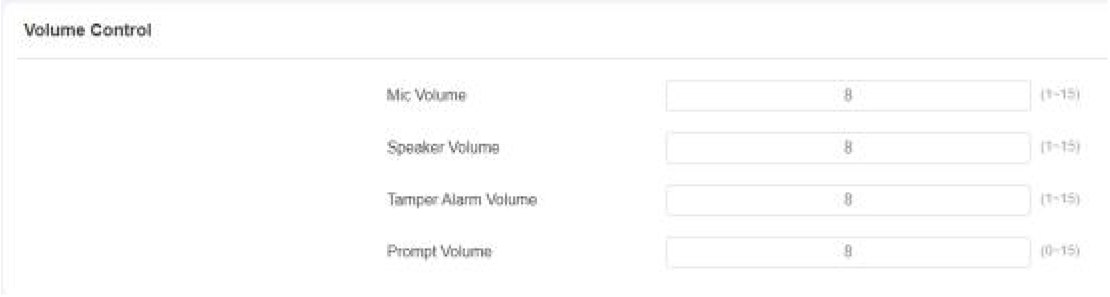


Parameter Set-up:

- **Mic Volume**: adjust the microphone volume according to your need.
- **Speaker volume**: adjust the loudspeaker volume according to your need.
- **PromptVolume:** adjust the prompt volume, which includes various types of prompt sound for door open success and failure, ringback, temperature measurement sound, etc.

5.5.1.2 Configure Volume on the Web Interface

On the web interface, you can set the temper alarm volume, Mic volume, speaker volume, and prompt volume. Path: **Device > Audio > Volume Control.**



Volume Control

Mic Volume: 8 (1-15)

Speaker Volume: 8 (1-15)

Tamper Alarm Volume: 8 (1-15)

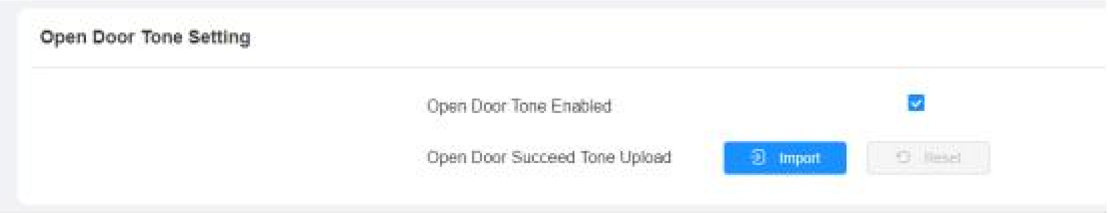
Prompt Volume: 8 (0-15)

Parameter Set-up:

- **Mic Volume:** set the mic volume from 1-15 according to your need. The default Mic volume is **8**.
- **Speaker Volume:** set the speaker volume from 1-15 according to your need. The default speaker volume is **8**.
- **Tamper Alarm Volume**: set the tamper alarm volume from 1-15 according to your need. The default volume is **8**.
- **PromptVolume:** adjust the prompt volume, which includes various types of prompt sound for door open success and failure, ringback, temperature measurement sound, etc.

5.5.2 Upload Open Door Tone

You can upload the Open-Door Tone on the device web interface. To configure the configuration on web **Device >Audio > Open Door Tone Setting**.



Open Door Tone Setting

Open Door Tone Enabled ☑

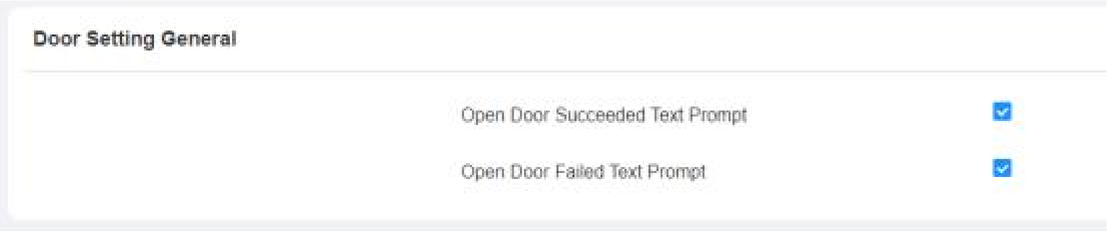
Open Door Succeed Tone Upload

Note

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

5.5.3 Configure Door Access Prompt Text

You can enable or disable the door access prompt to be shown on the access control terminal screen for door open failure and success. To configure the configuration on web **Setting > Door > Open Door Succeeded Text Prompt** interface.



Door Setting General

Open Door Succeeded Text Prompt ☑

Open Door Failed Text Prompt ☑

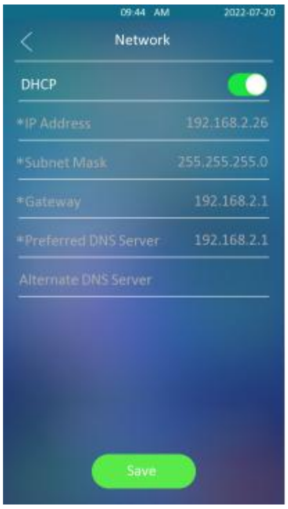
Parameter Set-up:

- **Open Door Success:** tick the check box if you want to see the text prompt after the door opening success.
- **Open Door Failed:** tick the check box if you want to see the prompt words after the door open failure.

6 Network Setting

6.1 Device Network Connection Setting

You can select DHCP (**Dynamic Host Configuration Protocol)** mode or static IP connection. When you select static IP connection, you can manually set up Subnet Mask, Default Gateway, and DNS servers.



DHCP ●

*IP Address 192.168.2.26

*Subnet Mask 255.255.255.0

*Gateway 192.168.2.1

*Preferred DNS Server 192.168.2.1

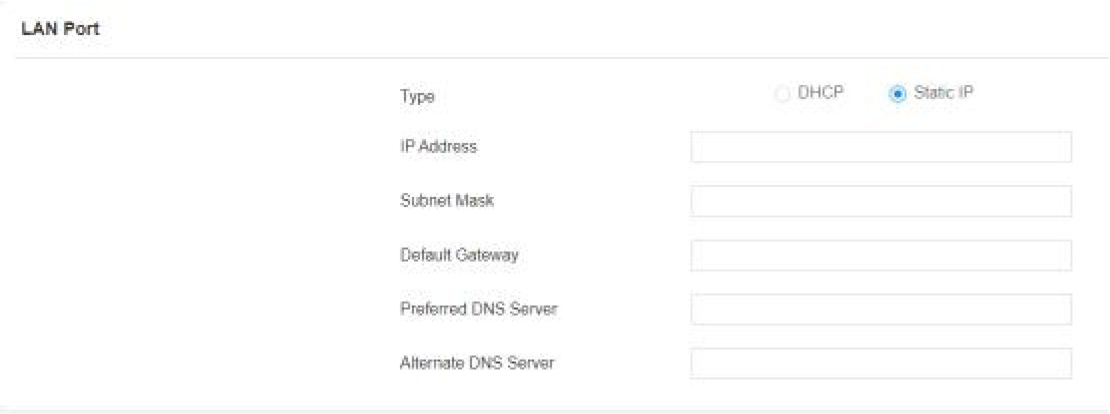
Alternate DNS Server

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**: select the **static IP mode** by checking off the DHCP check box. When static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS server address have to be manually configured according to your actual network environment.
- **IP Address**: set up the IP Address if the static IP mode is selected.
- **Subnet Mask**: set up the subnet Mask according to your actual network environment.

- **Gateway**: set up the correct gateway default gateway according to the IP address of the default gateway.
- **Preferred&Alternate DNS Server**: set up a preferred or 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.

To configure the device network on the web interface, go to **Network > Basic > LAN Port**.

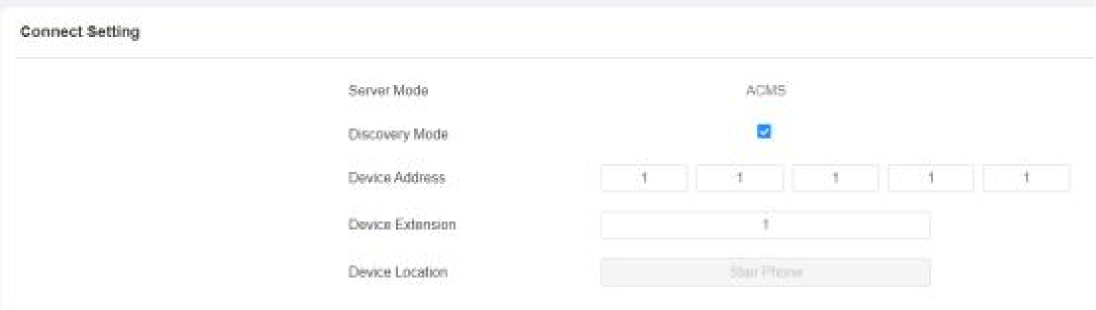


LAN Port

Type	○ DHCP ● Static IP
IP Address	
Subnet Mask	
Default Gateway	
Preferred DNS Server	
Alternate DNS Server	

6.2 Device Deployment in Network

E16C door phones should be deployed before they can be properly configured in the network environment in terms of their location, operation mode, address, and extension numbers as opposed to other devices for device control and the convenience of the management. To configure the configuration on web **Network > Advanced > Connect Setting** interface



Connect Setting

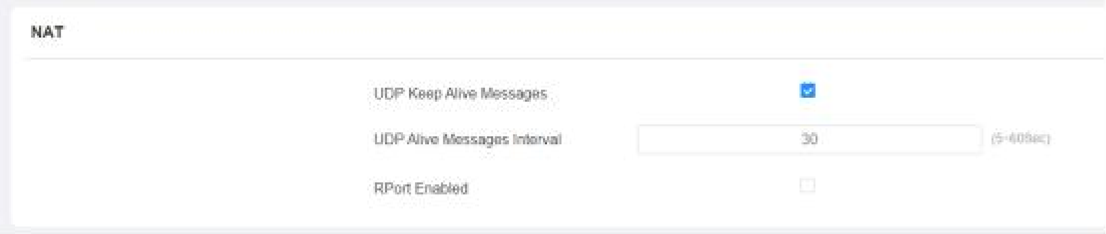
Server Mode	ACMS
Discovery Mode	☑
Device Address	1 1 1 1 1
Device Extension	1
Device Location	Stair Phone

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

6.3 NAT Setting

Network Address Translation (NAT) is what is used to map multiple local private addresses to legal public ones before transferring the information. To facilitate data transmission between the door phone and the SIP server, you will need to set up NAT. You can go to **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 the SIP server will recognize if the device is in online status.
- **UDP Alive Msg 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 AreaNetwork**).

7 Intercom Call Configuration

The intercom call in the device can be configured to allow you to perform a variety of customized intercom calls such as IP call and SIP call for different application scenarios.

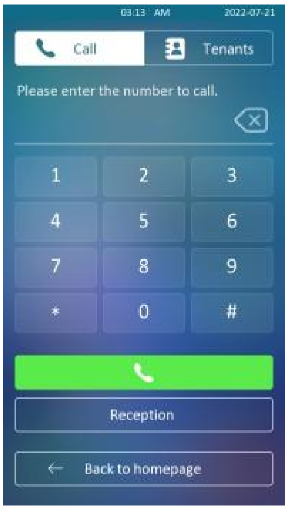
7.1 IP call & IP Call Configuration

IP calls can be made directly on the intercom device by entering the IP number on the device. And you can also disable the direct IP call if you allow no IP call to be made on the device.

7.1.1 Make IP calls

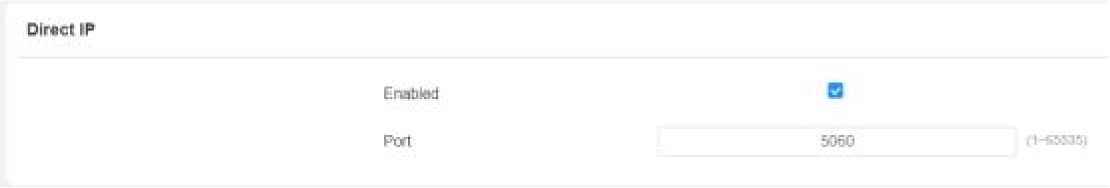
Preferred SIP Server

To make a direct IP call on the device, you can press the **Dial** 📞 icon, then enter the IP or SIP number and press the **Call** 📞 icon to call out.



7.1.2 IP Call Configuration

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



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 with.

7.2 SIP Call &SIP Call Configuration

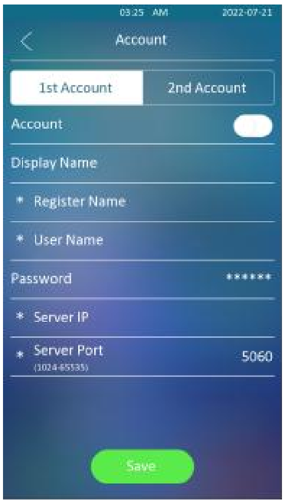
You can make a SIP call (**Session Initiation Protocol**) in the same way as you do for making the IP calls on the device. However, SIP call parameters related to its account, server, and transport type need to be configured first before you can make calls on the device.

7.2.1 SIP Account Registration

E16C supports two SIP accounts that can all be registered according to your applications. You can, for example, switch between them if any one of the accounts failed and become invalid. The SIP account can be configured on the device and on the device interface.

7.2.1.1 Configure SIP Account on the Device

On the device **Setting** screen, select **Account**.



Account

Display Name

* Register Name

* User Name

Password ******

* Server IP

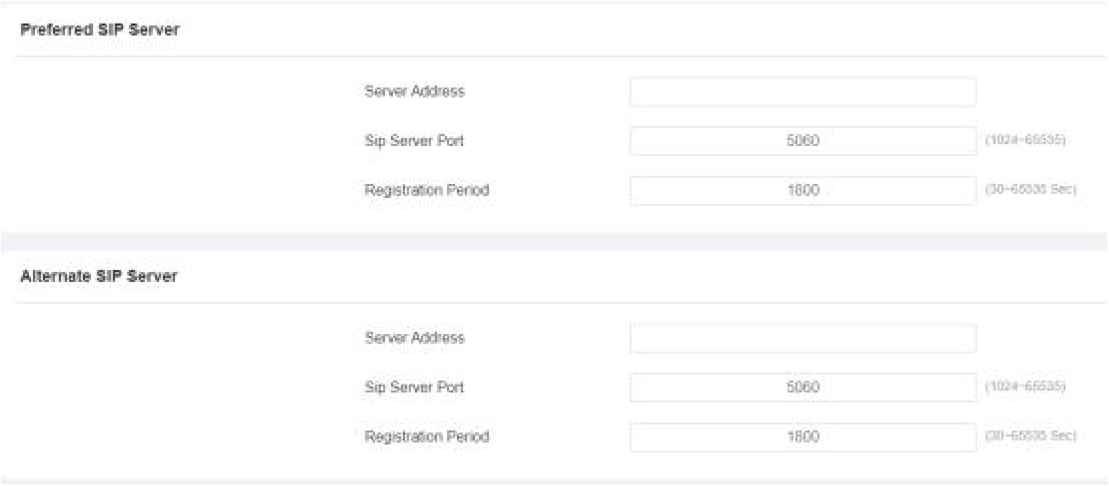
* Server Port (1024-65535) 5060

Parameter Set-up:

- **Status:** check to see if the SIP account is registered or not.
- **Account Active:** go to **Enable** or **Disable** to activate or deactivate the registered SIP account.
- **Display Name:** configure the name, for example, the device's name to be shown on the device being called to.
- **Display Label:** configure the device label to be shown on the device screen.
- **Register Name:** enter the SIP account register Name obtained from the SIP account administrator.
- **Username:** enter the user name obtained from the SIP account administrator.
- **Password:** enter the password obtained from the SIP account administrator.

7.2.2 SIP Server Configuration

SIP servers can be set up for devices in order to achieve call sessions through SIP servers between intercom devices. To set up a SIP server, you can go to **Account > Basic > Preferred SIP Server.**



Preferred SIP Server

Server Address

Sip Server Port 5060 (1024~65535)

Registration Period 1800 (30~65535 Sec)

Alternate SIP Server

Server Address

Sip Server Port 5060 (1024~65535)

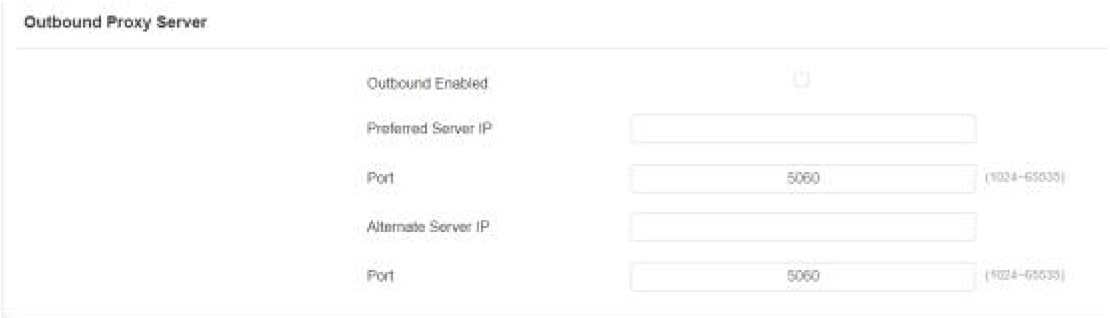
Registration Period 1800 (30~65535 Sec)

Parameter Set-up:

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

7.2.3 Configure Outbound Proxy Server

An outbound proxy server is used to receive all initiating request messages and route them to the designated SIP server in order to establish a call session via port-based data transmission. To configure the proxy server, you can go to **Account > Basic > Outbound Proxy Server**.



Outbound Proxy Server

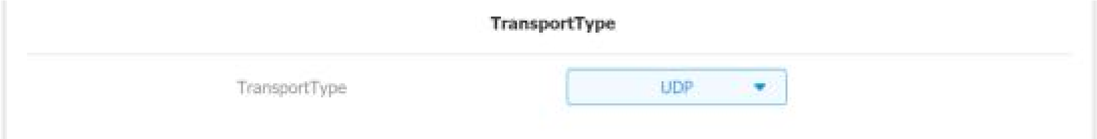
Outbound Enabled	□	
Preferred Server IP		
Port	5060	(1024~65535)
Alternate Server IP		
Port	5060	(1024~65535)

Parameter Set-up:

- **Outbound Enabled :** tick the checkbox to enable or disable the outbound proxy server.
- **Preferred Server IP:** enter the SIP address of the outbound proxy server.
- **Port:** enter the Port number for establishing a call session via the outbound proxy server.
- **AlternateServer IP:** set up Backup Server IP for the backup outbound proxy server.
- **Port:** enter the Port number for establishing a call session via the backup outbound proxy server.

7.2.4 Configure Data Transmission Type

SIP messages can be transmitted in three data transmission protocols: **UDP** (**User Datagram Protocol**), **TCP**(**Transmission Control Protocol**), **TLS** (**Transport Layer Security**), and **DNS-SRV.** In the meantime, you can also identify the server from which the data come. To do the configuration, you can go to **Account > Basic > Transport Type**.



TransportType

TransportType: UDP ▾

Parameter Set-up:

- **UDP**: select **UDP** for unreliable but very efficient transport layer protocol. UDP is the default transport protocol.

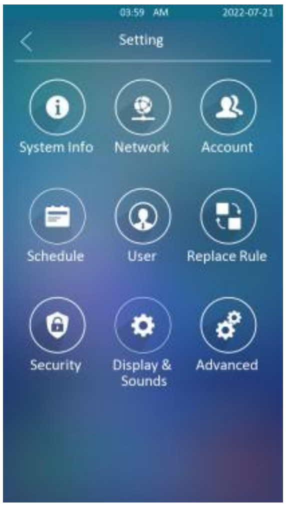
- **TCP**: select **TCP** for a reliable but less-efficient transport layer protocol.
- **TLS**: select **TLS** for Secured and Reliable transport layer protocol.
- **DNS-SRV**: select **DNS-SRV** to obtain a DNS record for specifying the location of servers. And **SRV** not only records the server address but also the server port. Moreover, SRV can also be used to configure the priority and the weight of the server address.

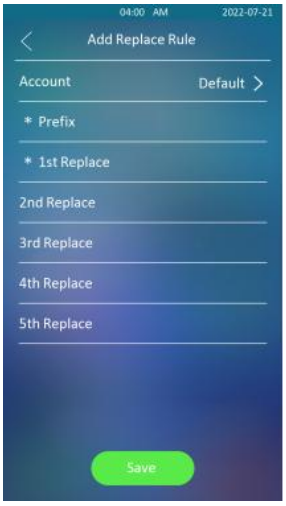
7.3 Dial Options Configuration

E16C offers a variety of Dial options that allows you to have a fast dial experience while relieving you of memory burden due to long and complex dial numbers.

7.3.1 Quick Dial By Number Replacement on the Device

You can replace multiple device dial numbers such as IP addresses or SIP numbers with only one short number. On the device Setting screen, select **Replace Rule**, then select **Add**.





Parameter Set-up:

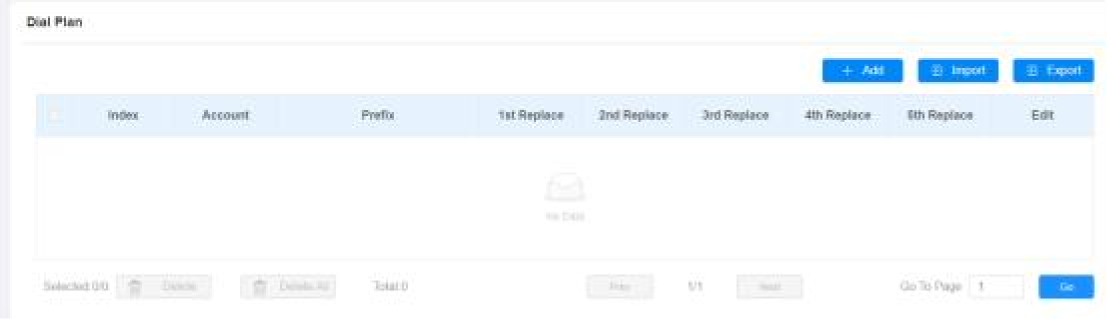
- **Account:** select the account to which you want to apply dial number replacement. The account is **Auto** by default (to dial out from the account in which the dialed number has been registered). You can select either account 1 or account 2 from which the number can be dialed out. If you have registered 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 numbers maximum for the replacement of 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**.

7.3.2 Quick Dial by Number Replacement on the Web Interface

You can replace the long SIP/IP number with the short number on the web interface. To configure it, you can go to **Intercom > Dial Plan**.



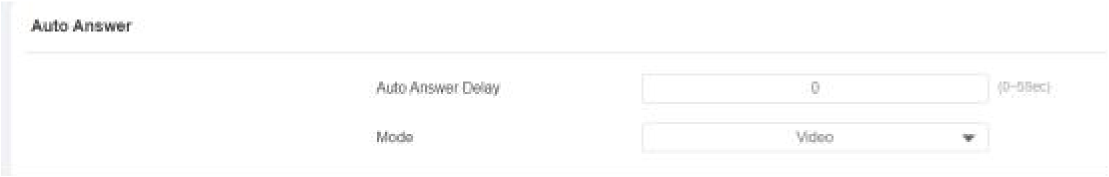
Index	Account	Prefix	1st Replace	2nd Replace	3rd Replace	4th Replace	5th Replace	Edit

7.4 Auto-answer Configuration

You set up the auto answer feature so that the door phone can automatically answer the incoming calls, such as, from the resident's indoor monitor, Smarplus App, and the guard phone. Also, you can select audio or video auto-answer mode based on your need.

To configure Auto-answer function:

Go to **Intercom > Call Feature > Auto Answer**.



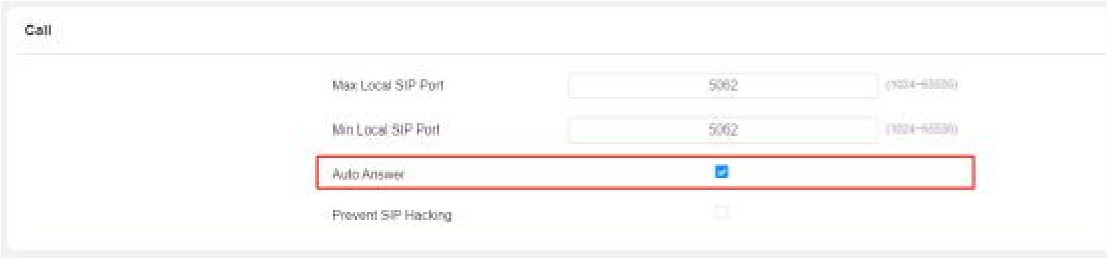
Auto Answer

Auto Answer Delay: 0 (0-5Sec)

Mode: Video

To enable Auto-answer mode:

Go to **Account > Advanced > Call**.



Call

Max Local SIP Port: 5062 (1024-65535)

Min Local SIP Port: 5062 (1024-65535)

Auto Answer: ☑

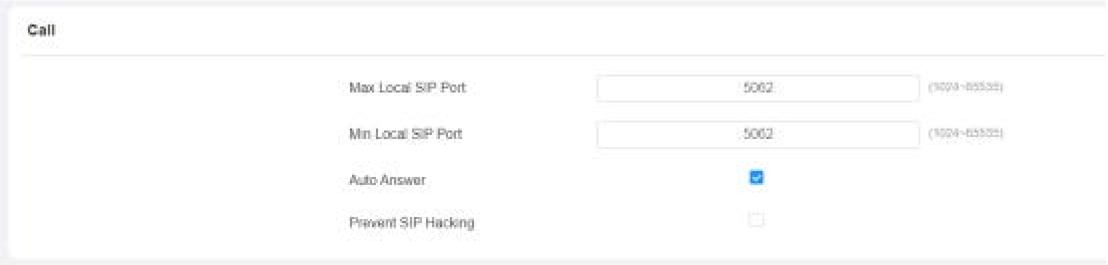
Prevent SIP Hacking: □

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.
- **Mode**: set up the **Video** or **Audio** mode you preferred for the automatic call answering.
- **Auto Answer:** enable the auto-answer function.

7.5 Enabling Prevent SIP Hacking

You can enable the Prevent SIP Hacking so that the door phone will only receive calls from the SIP numbers registered in the same SIP server, and contacts added locally or synchronized from Smartplus, SMDC, and ACMS.



Call

Max Local SIP Port 5062 (1024~65535)

Min Local SIP Port 5062 (1024~65535)

Auto Answer ☑

Prevent SIP Hacking □

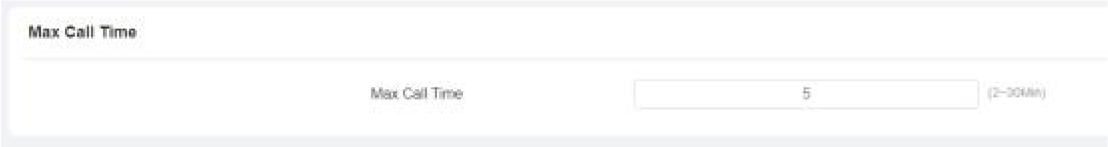
Note

The direct IP calls will be blocked if the direct IP is disabled.

7.6 Call Settings

7.6.1 Maximum Call Duration Setting

E16C door phone allows you to set up the call time duration in receiving the call from the calling party as the calling party might forget to hang up the phone. When the call time duration is reached, the door phone will terminate the call automatically. To do the configuration, you can go to **Intercom > Call Feature > Max Call Time**.



Max Call Time

Max Call Time 5 (2~30Min)

Parameter Set-up:

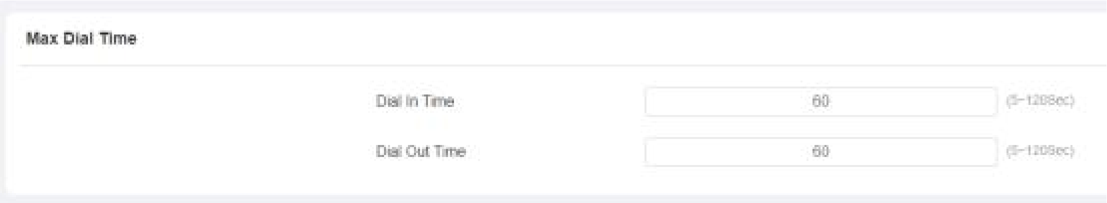
- **Max Call Time**: enter the call time duration according to your need (ranging from 2-30 min.). The default call time duration is 5 min.

Note

- The max call time of the device is also related to the max call time of SIP. If you use 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, then the SIP server max call time will be

7.6.2 Maximum Dial Duration Setting

Maximum Dial duration consists of the maximum dial-in time duration and the maximum dial-out time. Maximum dial-in time refers to the maximum time duration before the door phone hangs up the call if the call is not answered by the door phone. On the contrary, maximum dial-out time refers to the maximum time duration before the door phone hangs up itself automatically when the call from the door phone is not answered by the intercom device being called to. To do the configuration, you can go to **Intercom > Call Feature> Max Dial Time**.



Max Dial Time

Dial In Time: 60 (5~120Sec)

Dial Out Time: 60 (5~120Sec)

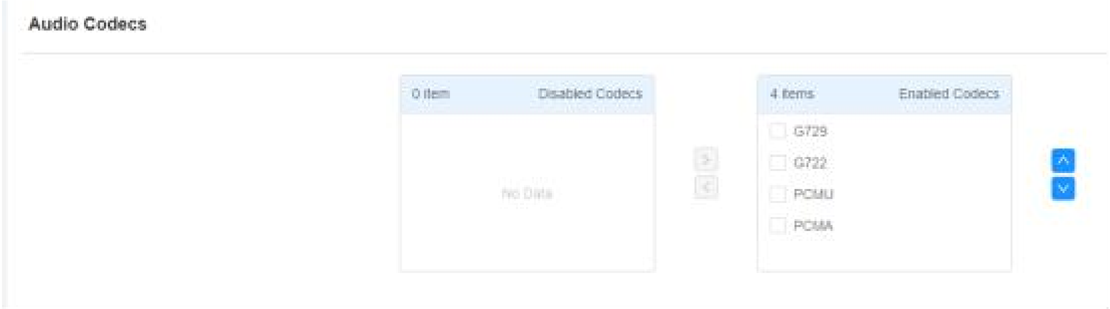
Parameter Set-up:

- **Dial In Time:** enter the dial-in time duration for your door phone (**ranging from 5-120 sec**). For example, if you set the dial-in time duration as 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 as 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.

7.6.3 Audio& Video Codec Configuration for SIP Calls

7.6.3.1 Configure Audio Codec

E16C door phones support four types of Codec (PCMU, PCMA, G729, G722) for encoding and decoding the audio data during the call session. Each type of Codec varies in terms of sound quality. You can select the specific codec with different bandwidths and sample rates flexibly according to the actual network environment. To do the configuration, you can go to **Account** > **Advanced > Audio Codecs.**


Audio Codecs

0 item	Disabled Codecs
No Data	

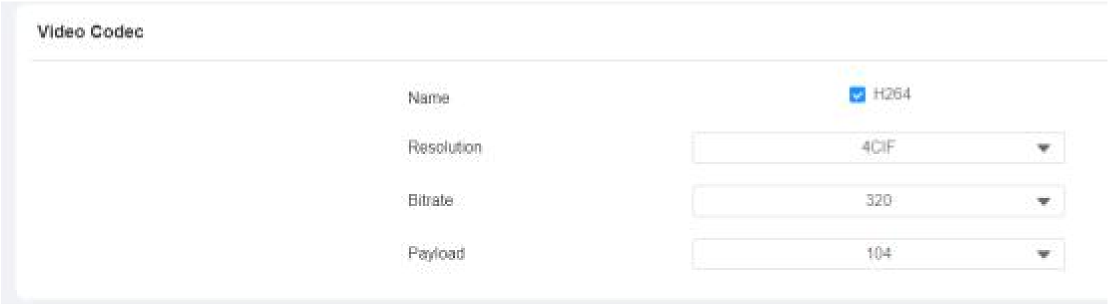
4 items	Enabled Codecs
□ G729	
□ G722	
□ PCMU	
□ PCMA	

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

7.6.3.2 Configure Video Codec

These series support the H.264 codec that provides a better video quality at a much lower bit rate with different video quality and payload. To do the configuration, you can go to **Account > Advanced > Video Codec.**



Video Codec

Name ☑ H264

Resolution 4CIF

Bitrate 320

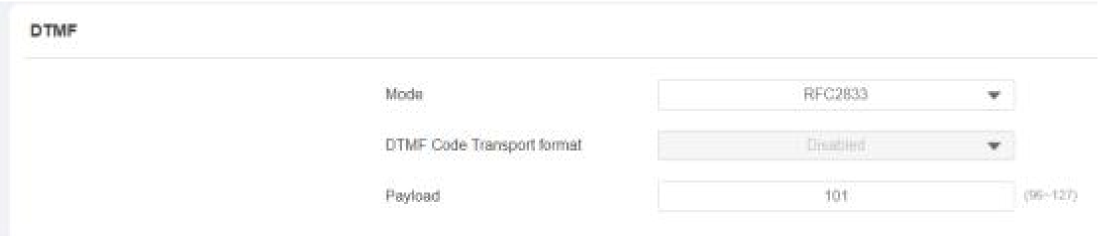
Payload 104

Parameter Set-up:

- **Name**: check to select the H264 video codec format for the door phone video H264 is the video codec by default.
- **Resolution:** select the code resolution for the video quality among four options: **QCIF, CIF, VGA, 4CIF, and 720P** according to your actual network environment. The default code resolution is 4CIF.
- **Bitrate:** select the video stream bit rate (ranging from 320-2048). The greater the bitrate, the data transmitted every second is greater in amount therefore the video will be clearer. While the default code bitrate is 2048.
- **Payload:** select the payload type (ranging from 90-118) 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.

7.7 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 the third-party integration. To configure the DTMF data transmission, you can go to **Account > Advanced > DTMF.**



DTMF

Mode RFC2833

DTMF Code Transport format Disabled

Payload 101 (96~127)

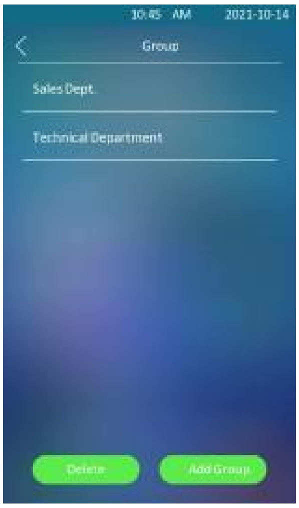
Parameter Set-up:

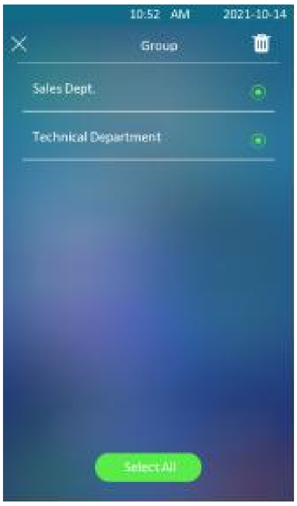
- **Mode:** select DTMF mode among five options: **Inband**, **RFC2833**, **Info+Inband,** and **Info+RFC2833** based on the specific DTMF transmission type of the third party device to be matched with as the party for receiving signal data.
- **How to Notify DTMF:** select among four types: **Disable**,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

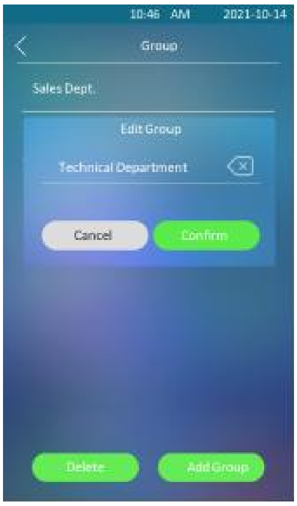
8 Contact List Configuration

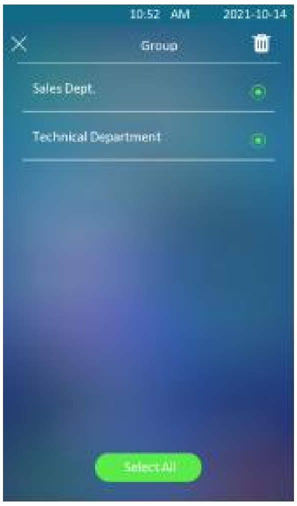
8.1 Contact List Configuration on the Device

You can configure the contact list in terms of adding and modifying contact groups or contacts on the device directly. To configure the phone book on the device **User > Group.**





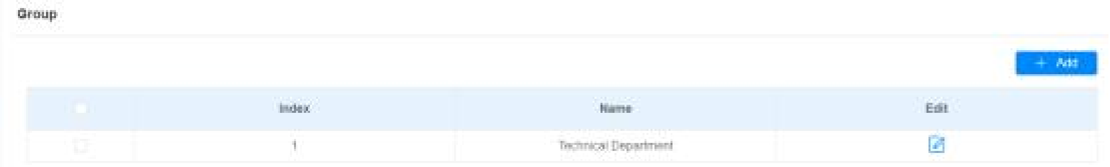




8.2 Contact List Configuration on the Web Interface

8.2.1 Managing Contact Groups on the Web Interface

You can configure contact and contact groups by adding and editing them on the web **Directory > User > Group** interface.

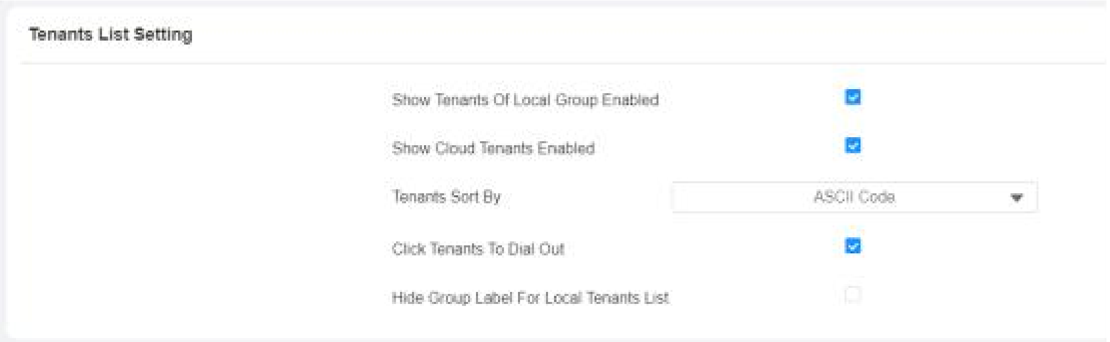


Group

□	Index	Name	Edit
□	1	Technical Department	✎

8.2.2 Managing Contact List Display Setting

If you want to customize your contact list displayed to your desired visual preference, you can go to **Directory > Directory Setting> Tenants List Setting.**



Tenants List Setting

Show Tenants Of Local Group Enabled	☑
Show Cloud Tenants Enabled	☑
Tenants Sort By	ASCII Code ▾
Click Tenants To Dial Out	☑
Hide Group Label For Local Tenants List	□

Parameter Set-up:

- **Show Tenants of Local Group 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 tenant's list. And when you untick the check box, the cloud tenants will be hidden.
- **Tenants Sort By:** select **ASCII Code or Room No.** or **Import**. When you select ASCII Code, the tenants will be listed by their names in the sequence of the ASCII code. When you select Room No., the tenants will be sorted according to their room

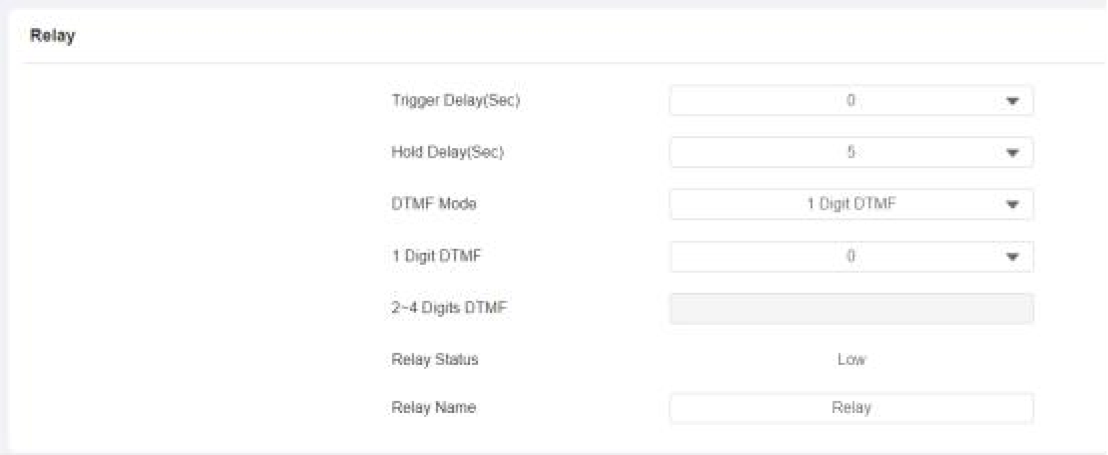
numbers. This is applicable to the local contacts and contacts synchronized from the SmartPlus cloud.

- **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 in the middle of the tab to dial out.
- **Hide Group Label for Contact List:** tick or untick the check box to control the display of the group label. If you untick the check box, then only the contact tab will be displayed while the group tab will be concealed and vice versa.

9 Relay Switch Setting

9.1 Relay Switch Setting

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



Relay

Trigger Delay(Sec)	0
Hold Delay(Sec)	5
DTMF Mode	1 Digit DTMF
1 Digit DTMF	0
2-4 Digits DTMF	
Relay Status	Low
Relay Name	Relay

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 the **Unlock** tab**.**
- **Hold Delay (Sec):** set the relay hold delay timing (ranging from 1-10 Sec). For example, if you set the hold delay time as 5 sec, then the relay will stay triggered for 5 seconds after the door is It means the door will stay open for 5 seconds.
- **DTMF Mode:** select the number of DTMF digits for the door access control (**Ranging from 1-4 digits**) For example, you can select a 1-digit DTMF code or 2-digit DTMF code, etc., according to your need.
- **1-Digt DTMF:** set the 1-digt DTMF code within range from (**0-9 and *, #**).
- **2~4 Digits DTMF:** set the DTMF code according to the **DMTP Option**. For example, you are required to set the 3-digits DTMF code if DTMP Mode is set as 3-digits.

- **Relay Status:** relay status is low by default which means normally closed (NC). If the relay status is high, then it is in normally open status (NO).
- **Relay Name:** name the relay switch according to your need. For example, you can name the relay switch according to where the relay switch is located for convenience.

Note

- Only the external devices connected to the relay switch need to be powered by powered adapters as the relay switch does not supply power.

Note

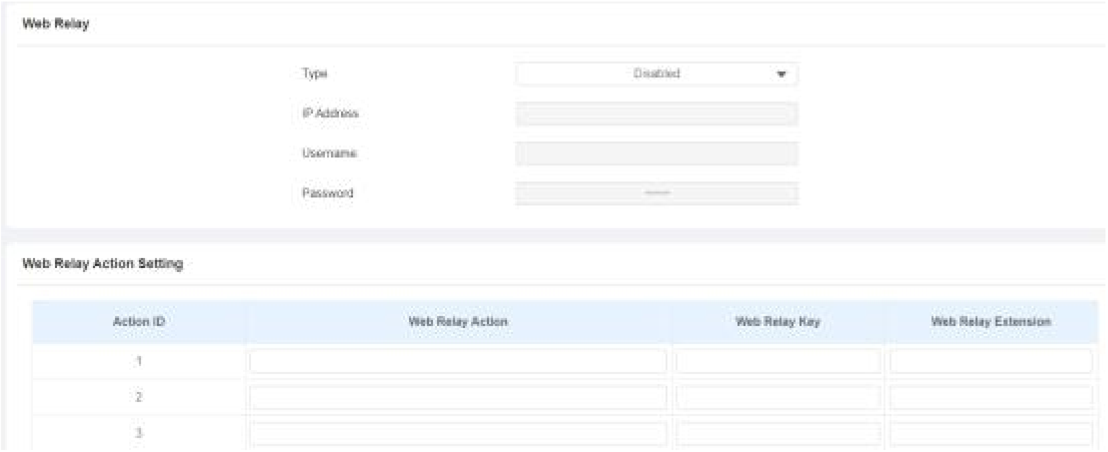
- If DTMF mode is set as **1 Digit DTMF**, you cannot edit DTMF code in **2~4 Digits DTMF** and if you set DTMF mode from 2-4 in **2~4 Digits DTMF** field, you cannot edit DTMF code in **1 Digit DTMF** field.

9.2 Web Relay Setting

In addition to the relay that is connected to the door phone, you can also control the door access using the network-based web relay on the device and on the device web interface.

9.2.1 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, and password. And you can fill in a maximum of 50 web relay action commands for different web relay actions, which can later be selected on the device screen for the specific relay action for the door access control. Path: **Access Control > Web Relay.**



Web Relay

Type	Disabled
IP Address	
Username	
Password	

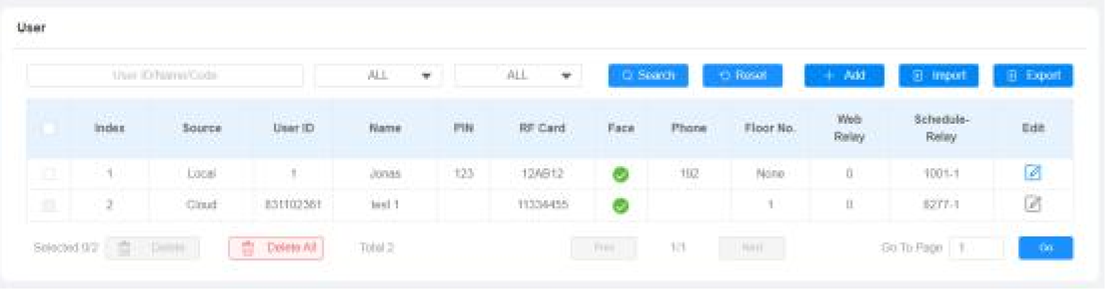
Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
1			
2			
3			

Parameter Set-up:

- **Type:** among three options **Disabled**, **WebRelay** and **Both**. Select **WebRelay** to enable the web relay. Select **Disable** to disable the web relay. Select **Both** to enable both local relay and web relay. If you select Web relay, then the local relay will not be valid.
- **IP Address:** enter the web relay IP address provided by the web relay manufacturer.
- **User Name**: enter the User name provided by the web relay manufacturer.
- **Password:** enter the password provided by the web relay manufacturer. The passwords are authenticated via HTTP and you can define the passwords using **http get** Action.
- **Web Relay Action:** enter the specific web relay action command provided by the web manufacturer for different actions by the web relay.
- **Web Relay Key:** enter the configured DTMF code, when the door is unlocked via the DTMF code, the action command will be sent to the web relay automatically.

After the web relay is set up, you can select the specific web relay action to be carried out. You can go to **Directory > User,** then click + Add , then scroll down to **Access Setting**.

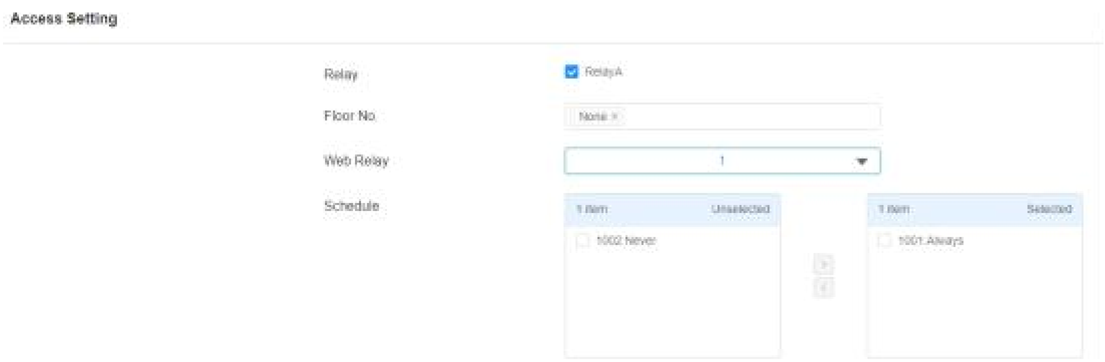


User

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	Jonas	123	12AB12	✓	102	None	0	1001-1	✎
□	2	Cloud	831102361	test 1		11334455	✓		1	0	8277-1	✎

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

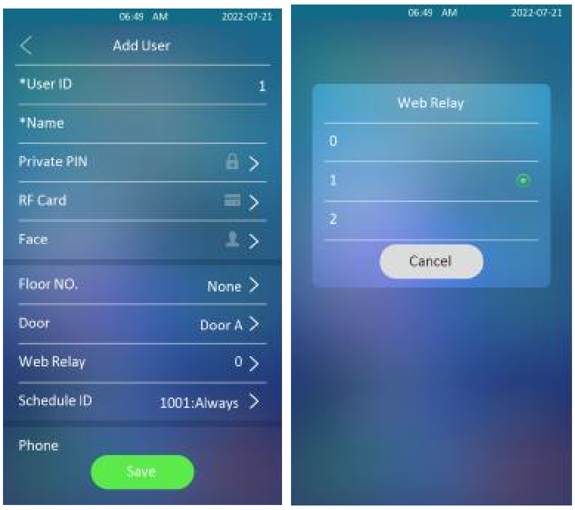


Access Setting

Relay	☑ RelayA
Floor No	None ×
Web Relay	1
Schedule	1 item Unselected: □ 1002:Never 1 item Selected: □ 1001:Always

9.2.2 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. To configure it, go to **User > User List.**



06:49 AM 2022-07-21

Add User

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

Save

06:49 AM 2022-07-21

Web Relay

0

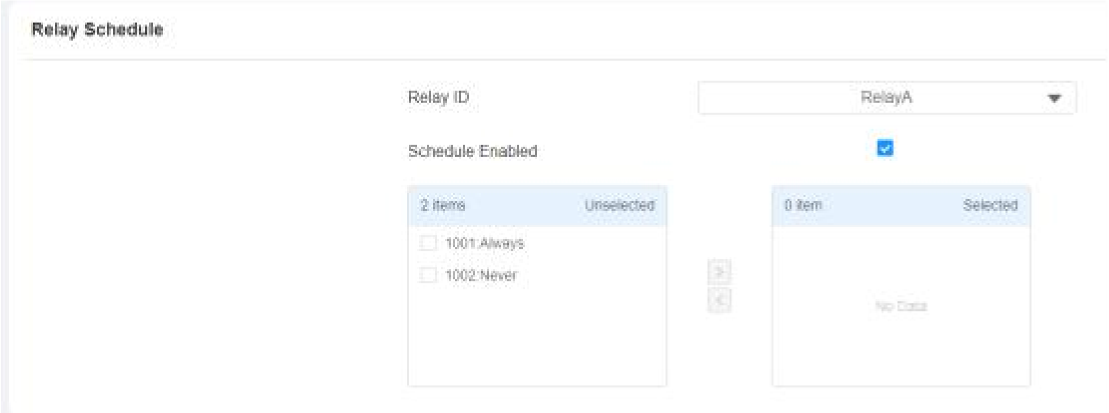
1 ●

2

Cancel

9.3 Relay Schedule

Set the corresponding relay always open at a specific time. This feature is designed for some specific scenarios, such as, the time after school, or for morning work time. To do the configuration, navigate to **Access Control > Relay > Relay Schedule**interface.



Relay Schedule

Relay ID: RelayA

Schedule Enabled: ☑

2 items Unselected
□ 1001:Always
□ 1002:Never

0 item Selected
No Data

Parameter Set-up:

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

Note

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

10 Door Access Schedule Management

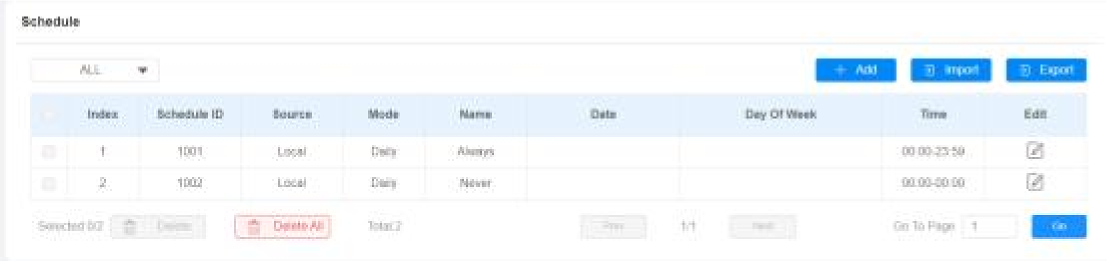
You are required to configure and make a schedule for the user-based door access via RF card, private PIN, and facial recognition.

10.1 Configure Door Access Schedule

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

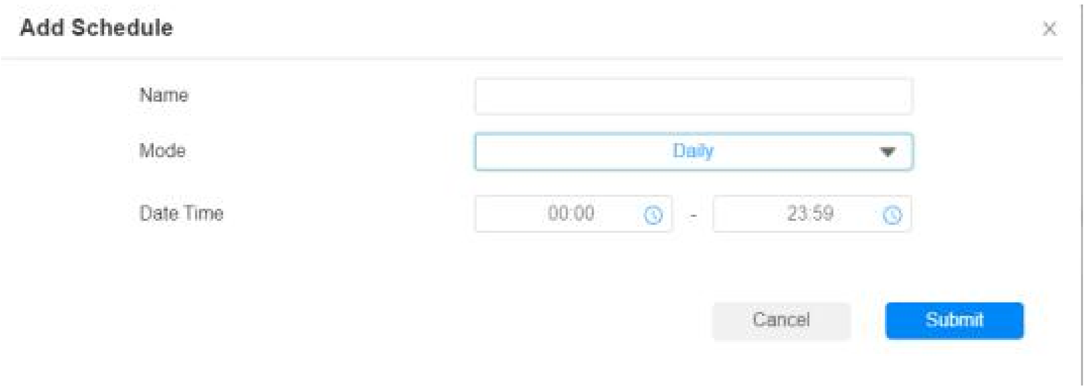
10.1.1 Create Door Access Schedule on the Web

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 .



	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	

To create a daily schedule, select **Daily** mode.

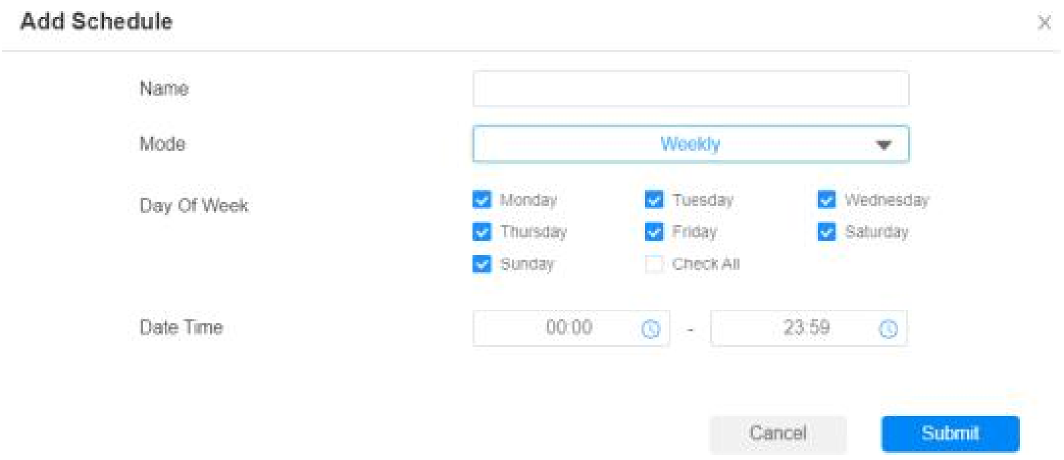

Add Schedule

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

Parameter Set-up:

- **Mode**: select daily schedule.
- **Name:** enter the daily schedule name.
- **Date Time**: set up the time schedule for the validity of the door access during the day.

To create a daily schedule, select **Weekly** mode.



Add Schedule

Name

Mode: Weekly

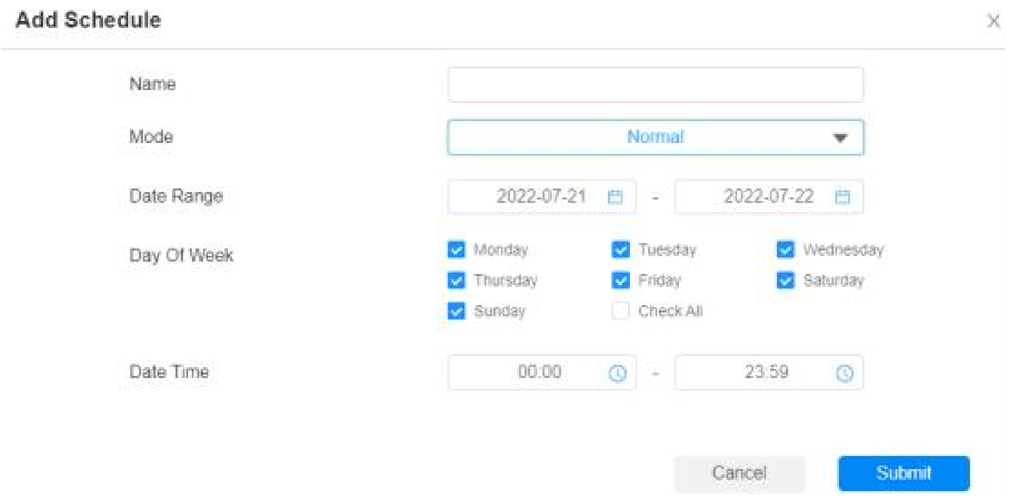
Day Of Week: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday □ Check All

Date Time: 00:00 - 23:59

Parameter Set-up:

- **Day of Week:** select the day (s) on which door access can be valid on a weekly.

To create a longer period schedule:



Add Schedule

Name

Mode: Normal

Date Range: 2022-07-21 - 2022-07-22

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

Date Time: 00:00 - 23:59

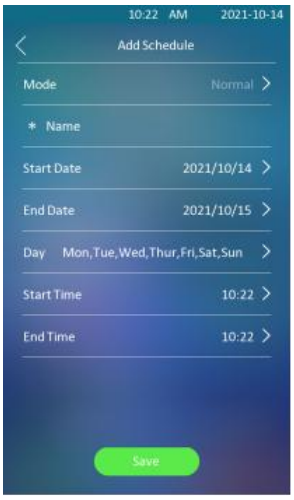
Cancel Submit

Parameter Set-up:

- **Start Date- End Date**: set the date range of the validity of the door access.

10.1.2 Create Door Access Schedule on the Device

You can also create a door access schedule on the device. You can go to **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

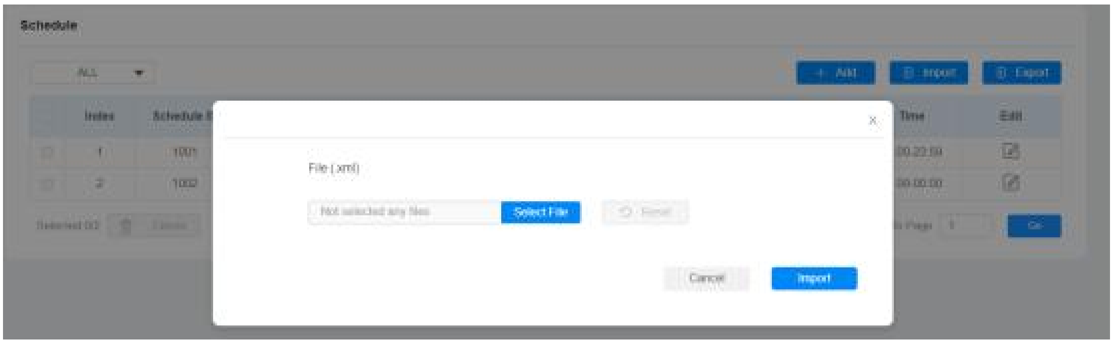
Start Time: 10:22

End Time: 10:22

Save

10.1.3 Import and Export Door Access Schedule

In addition to creating door access a schedule separately, you can also conveniently import or export the schedules in order to maximize your door access schedules management efficiency. You can go to **Setting > Schedule**, then click **Import**.



File (.xml)

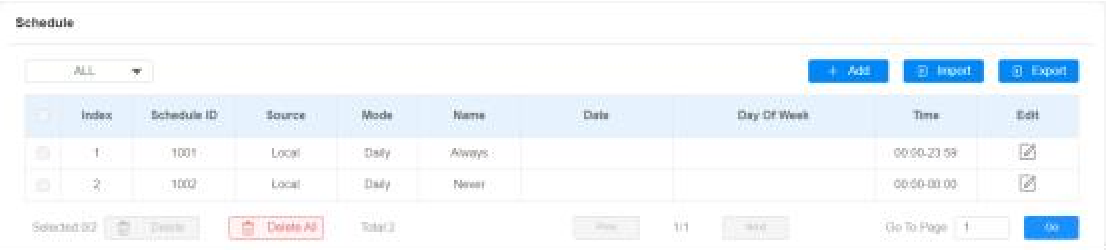
Not selected any files | Select File | Reset

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

10.1.4 Edit the Door Access Schedule

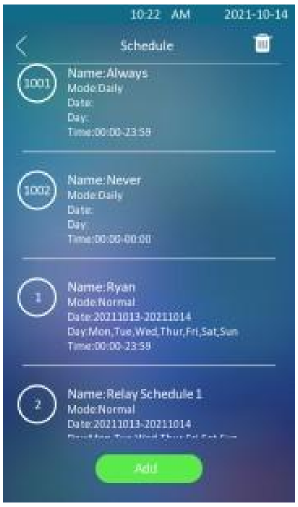
If you want to edit or delete the door access schedule you created, you can edit or delete the configured schedule separately or in batch.

To edit the schedule on the web interface, go to **Setting > 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	

To edit the schedule on the device, tap Schedule, then tap the schedule you want to edit.



10:22 AM 2021-10-14

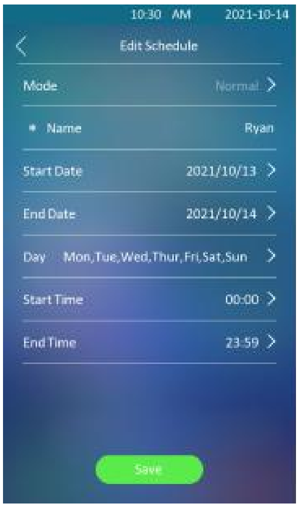
Schedule

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



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

Note

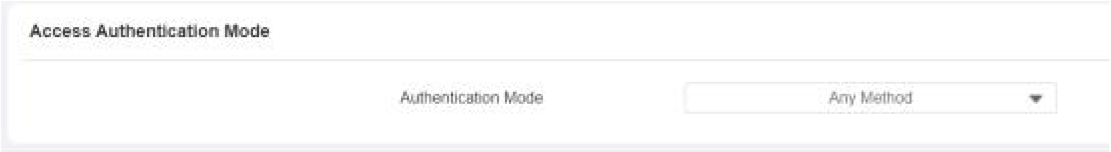
- It only supports .xml format files for importing and exporting the schedule.

11 Door Unlock Configuration

E16C door phones offer you three types of door access via PIN code, RF card, and Facial recognition. You can configure them on the device and web interface. Moreover, you can import or export the configured files to maximize your RF card configuration efficiency.

11.1 Access Authentication

You can set up several access authentication modes, and set up authentication security as needed. On the web, navigate to **Access Control > Relay > Access Authentication Mode**.



Access Authentication Mode

Authentication Mode: Any Method

Parameter Set-up:

- **Authentication Mode**: select **Any method** if you allow all the access methods to unlock the door. Select **Face + PIN** if you want to apply dual access methods (Face + PIN) for the door unlock. Select **Face + RF Card** if you want to apply dual access methods (Face+ RF Card) for the door unlock.

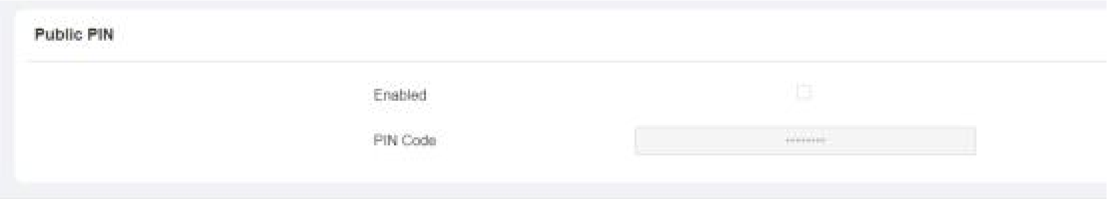
11.2 Configure PIN Code for Door Unlock

You can create and modify both public PIN codes and private PIN codes for door access on E16C door phones.

11.2.1 Configure Public PIN code

You can configure and change public PIN codes.

On the web interface, go to **Access Control > PIN Setting > Public PIN.**



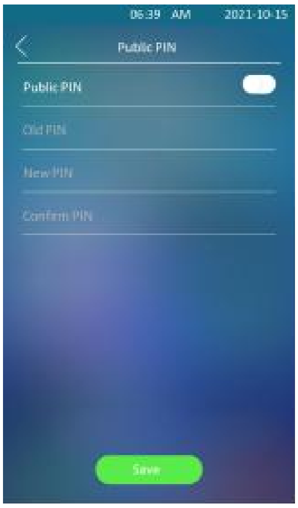
Public PIN

Enabled □

PIN Code ••••••••

Parameter Set-up:

- **Enabled**: tick the check box to enable the Public PIN code application.
- **PIN Code**: set the PIN code with a digit limit ranging from **4-8**.



06:39 AM 2021-10-15

Public PIN

Public PIN

Old PIN

New PIN

Confirm PIN

Note

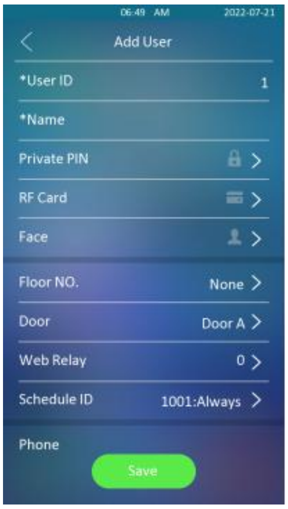
- The public PIN code will not be valid until the function is turned on.

Note

- **APT+PIN** is applicable only when the device is added to the Akuvox SmartPlus.

11.2.2 Configure Private PIN Code on the Device

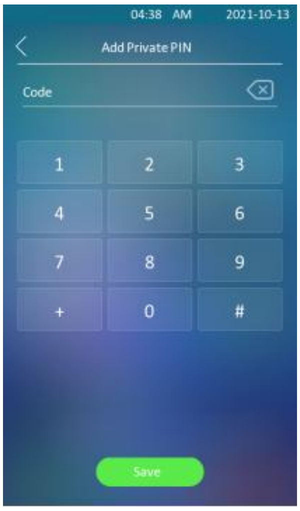
You can configure door access by Private PIN code for the resident on the device by entering the user's name and the PIN code for the door access. Path: **User > User List.**



06:49 AM 2022-07-21

Add User

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



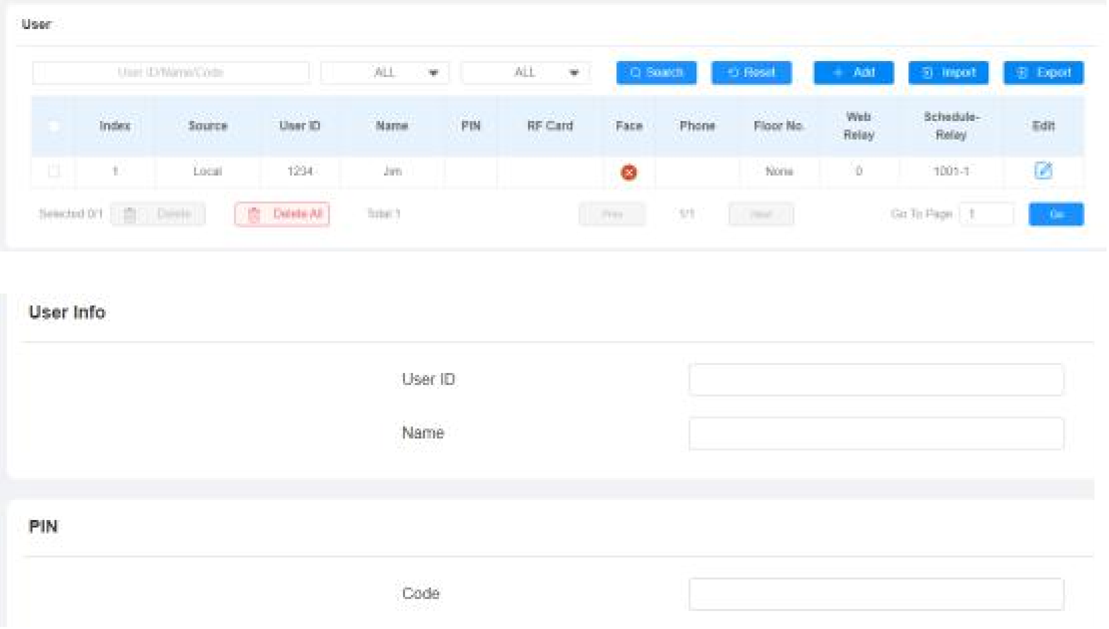
04:38 AM 2021-10-13

Add Private PIN

Code

11.2.3 Configure Private PIN Code on the Web Interface

On the web interface, you can not only set up a PIN code but also set and select the door access schedule that you created for the validity of the PIN Code access during a certain time span you scheduled. In addition, you can set the limit for the total number of valid PIN code door access. To configure the PIN code, go to **Directory > User** interface.



User

□	Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
□	1	Local	1234	Jim			⊗		None	0	1001-1	✎

User Info

User ID	
Name	

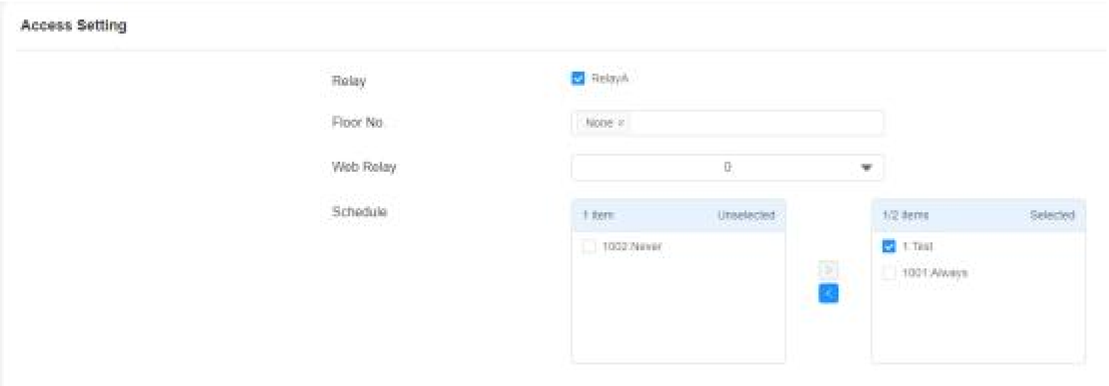
PIN

Code	

Parameter Set-up:

- **User ID**: enter the user's ID.
- **Name**: enter the user name (resident's name).
- **Code**: enter the user's private PIN.

After user information and PIN code are entered, you can scroll down to **Access Setting** on the same page to set door access Schedule for Private PIN Code door access:



Access Setting

Relay ☑ RelayA

Floor No None ×

Web Relay 0

Schedule

1 item Unselected
□ 1002 Never

1/2 items Selected
☑ 1 Test
□ 1001 Always

Parameter Set-up:

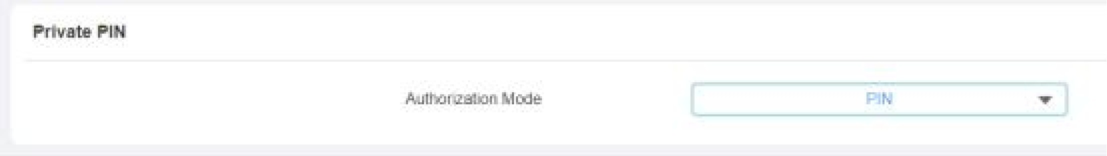
- **Relay:** select the relay for the door unlock for the user.
- **Floor NO:** enter the resident's floor number.
- **Web relay:** select the specific number of web relay action commands you have set up on the web interface.
- **Schedule:** select from the created door access schedule on the right box 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 as they are identical in configuration.

11.2.4 Configure Private PIN Access Mode

E16C offers you two types of access modes for private PIN code access, namely **PIN** and **APT#+PIN**. Path: **Access Control > PIN Setting > Private PIN.**



Private PIN

Authorization Mode: PIN

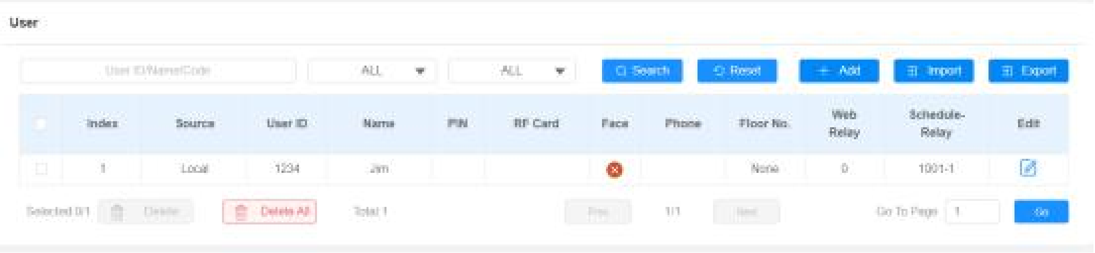
Parameter Set-up:

- **Authorization Mode:** select access mode between **PIN** and **APT#+PIN**. If you select the **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.

11.3 Configure RF Card for Door Unlock

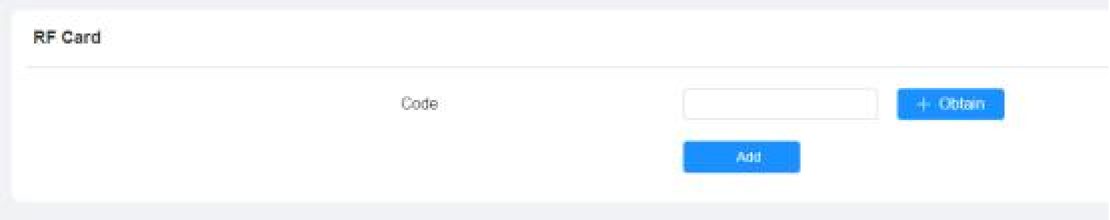
11.3.1 Add RF Card on the Web Interface

To add RF cards, go to **Directory > User**, then click + Add .



User

□	Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
□	1	Local	1234	Jim			⊗		None	0	1001-1	✎



RF Card

Code

Note

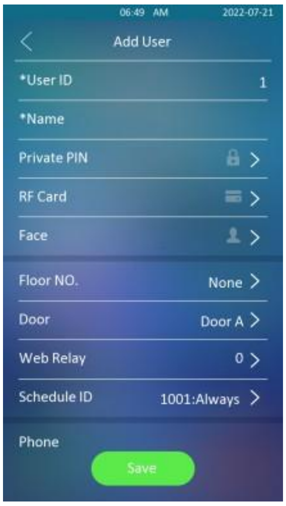
- Please refer to PIN code access schedule selection for the RF card user(s)-specific door access.

Note

- RF card with 13.56 MHz and 125 KHz can be applicable to the door phone for door access.

11.3.2 Add RF Card to the Device

You can configure the RF card directly on the device for the door access while setting up the time schedule for the validity of the RF card access along with the web relay that can be triggered with the RF card etc. To add an RF card, tap **User**, then **User List**, then **Add**.



06:49 AM 2022-07-21

Add User

*User ID 1

*Name

Private PIN

RF Card

Face

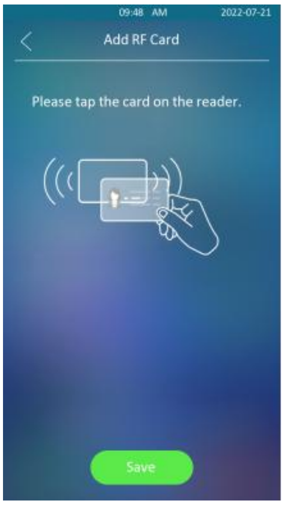
Floor NO. None

Door Door A

Web Relay 0

Schedule ID 1001:Always

Phone



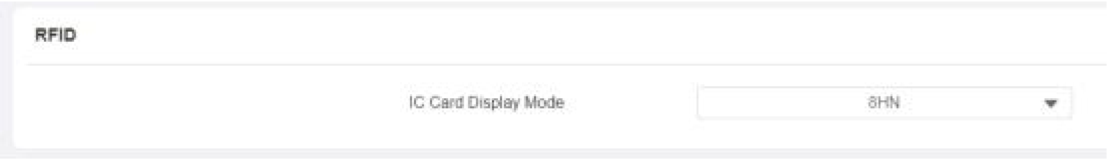
09:48 AM 2022-07-21

Add RF Card

Please tap the card on the reader.

11.3.3 Configure RF Card Code Format

If you want to integrate with the third-party intercom system in terms of RF card door access, you can change the RF card code format to be identical to that applied in the third-party system. To configure the configuration on the web **Access Control > Card Setting** interface.



RFID

IC Card Display Mode: 8HN

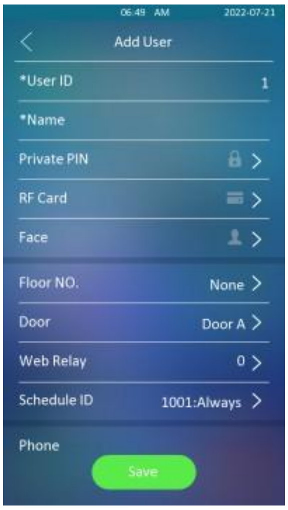
Parameter Set-up:

- **IC-Card Display Mode**: select the card format for the **ID Card** for the door access among five format options: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR.** The card code format is 8HN by default in the door phone.

11.4 Configure Facial Recognition for Door Unlock

11.4.1 Enroll Face Data on the Device

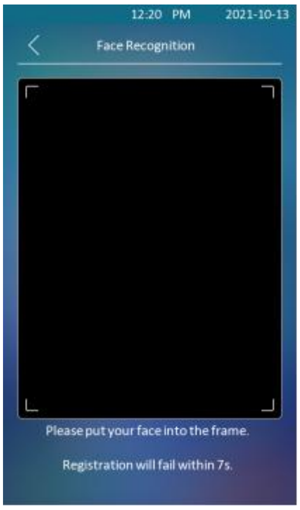
You can configure door access by facial recognition on the device by entering the user's name and registering your facial ID on the device for door access. Tap **User > User List,** then tap Add, and tap **Face**.



06:49 AM 2022-07-21

Add User

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



12:20 PM 2021-10-13

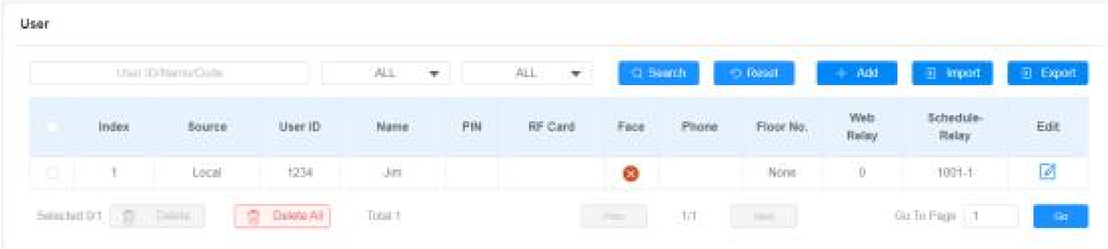
Face Recognition

Please put your face into the frame.

Registration will fail within 7s.

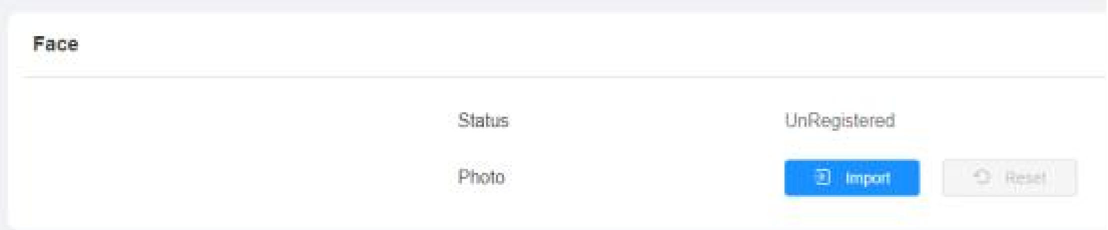
11.4.2 Upload Face Data on the Web Interface

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	1234	Jim			☒		None	0	1001-1	✎



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**.

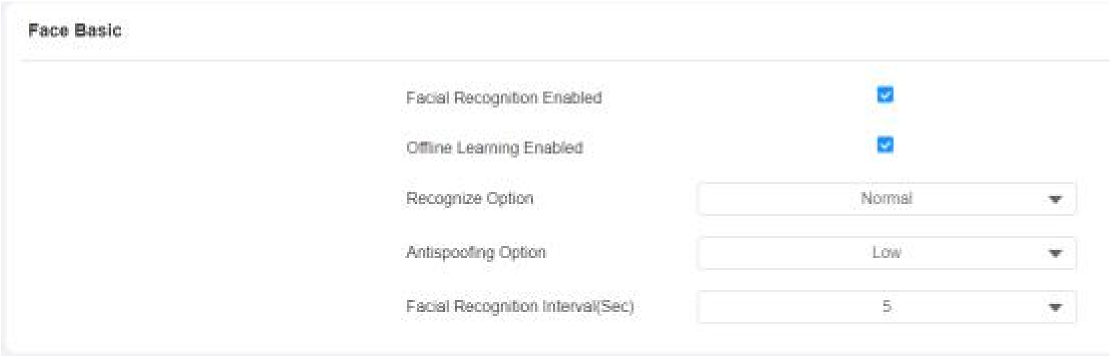
- **Photo(jpg/png):** select the picture with jpg or png format to be uploaded to the device and press if you want to clear the picture uploaded.

Note

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

11.4.3 Configure Facial Recognition

E16C door phones allow you to adjust facial recognition accuracy, and recognition intervals according to your actual need. And you can also improve the recognition quality and user experience through the basic facial recognition setting. To configure the configuration on the web **Access Control > Face Setting** interface.



Face Basic

Facial Recognition Enabled ☑

Offline Learning Enabled ☑

Recognize Option: Normal

Antispoofing Option: Low

Facial Recognition Interval(Sec): 5

Parameter Set-up:

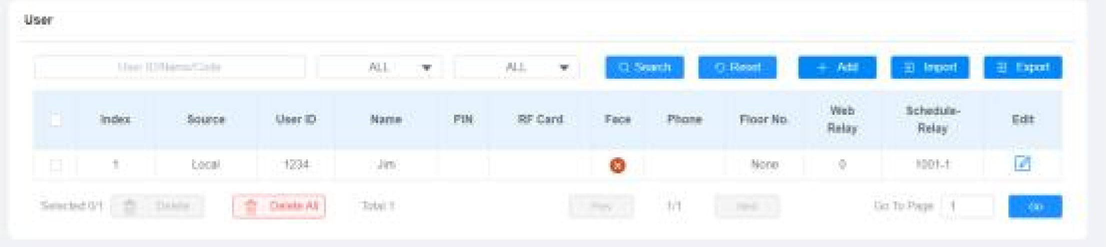
- **Face RecognitionEnabled:** click on **Enable** to turn on the facial recognition function. Facial recognition is enabled by default.
- **Offline LearningEnabled:** select **Enable** if you want to improve the device recognizing capability, focusing on the major facial characteristics while sidelining the minor changes that occurred to your face. Facial recognition accuracy improves as the number of facial recognition increases.
- **Recognize Option:** click to select the facial recognition accuracy level among four options: **Low, Normal, High,** and **Highest.** For example, if you select **Highest** then

there will be the least possibility that someone else will be mistaken for you by mistake or in another way round in the facial recognition.

- **Antispoofing OptionEnabled:** select Anti-spoofing level among four options: **Low, Normal, High, 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 minutes. For example, if you select **5** then you have to wait for 5 min. before you are allowed to perform the facial recognition again.

11.5 Configure Door Access Using Configured Files

E16C door phones allow 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 settings 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. You can go to **Directory > User** interface.



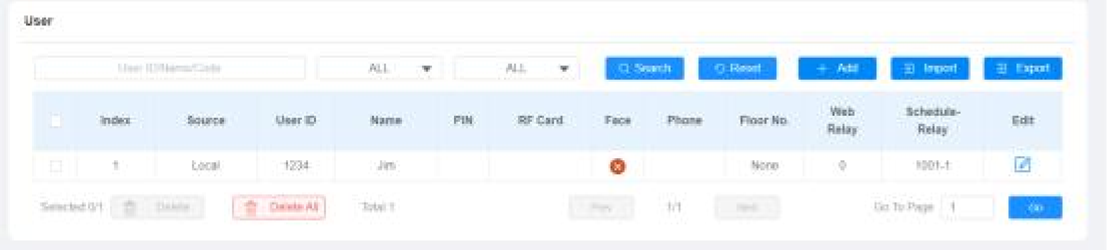
□	Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
□	1	Local	1234	Jim			☒		None	0	1001-1	✎

Note

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

11.5.1 Editing the User(s)-specific Door Access Data

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

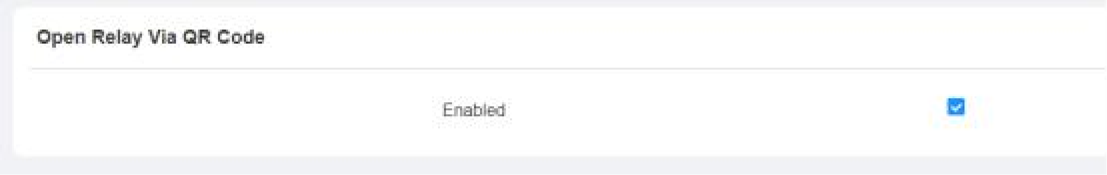


User

☐	Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
☐	1	Local	1234	Jim			☒		None	0	1001-1	✎

11.6 Unlock by QR Code

QR code is another option for door unlock. You need to enable the QR code function before you can gain door unlock via QR code. You can go to **Access Control > Relay > Open Relay via QR Code**.



Open Relay Via QR Code

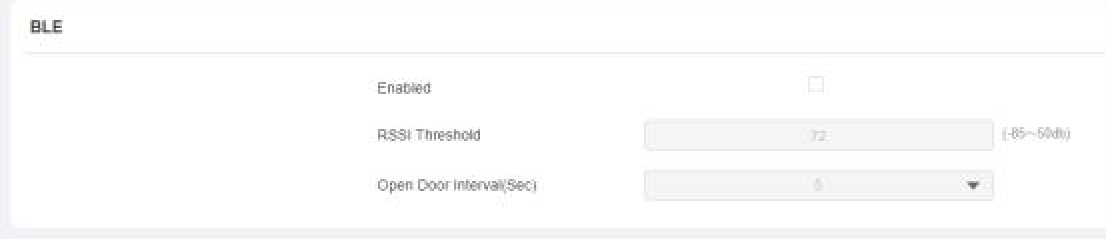
Enabled ☑

Note

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

Unlock by Bluetooth

You can also gain the door access by mobile phone with Bluetooth which is used together with Akuvox SmartPlus. You can shake the mobile phone closer to the access control terminal for the door access. To configure the configuration on web **Access Control > BLE > BLE** interface.



BLE

Enabled ☐

RSSI Threshold 72 (-85~50db)

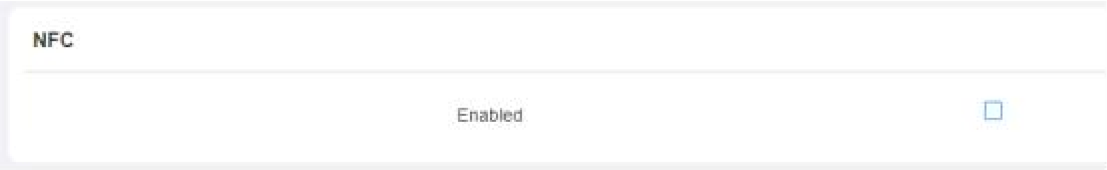
Open Door Interval(Sec) 5

Parameter Set-up:

- **Enabled:** enable or disable the Bluetooth. Bluetooth is turned off by default.
- **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:** select the time interval between every two Bluetooth door accesses.

11.7 Unlock by NFC

You can also gain door access by mobile phone with NFC which is used together with Akuvox SmartPlus. You can keep the mobile phone closer to the door phone for door access. Path: **Access Control > Card Setting> NFC.**


NFC

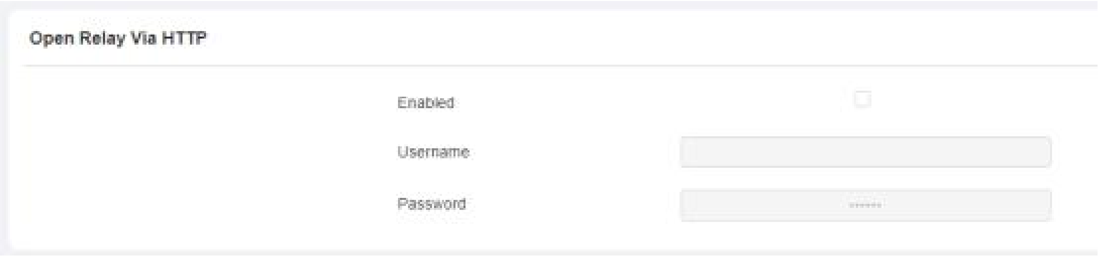
Enabled □

Parameter Set-up:

- **Enable:** enable the NFC function if you want to unlock the door via NFC.

11.8 Unlock by HTTP Command on Web Browser

You can unlock the door remotely without approaching the device physically for the door access by typing in the created HTTP command (URL) on the web browser to trigger the relay when you are not available by the door for the door access. To configure the configuration on web **Access Control > Relay > Open Relay via HTTP** interface.


Open Relay Via HTTP

Enabled □

Username

Password ······

Parameter Set-up:

- **Enabled:** enable the HTTP command to unlock the function by going to **Enable**.
- **Username:** enter the user name of the device web interface, forexample, **Admin**.
- **Password**: enter the password for the HTTP command. For example, **12345**.

Please refer to the following example:

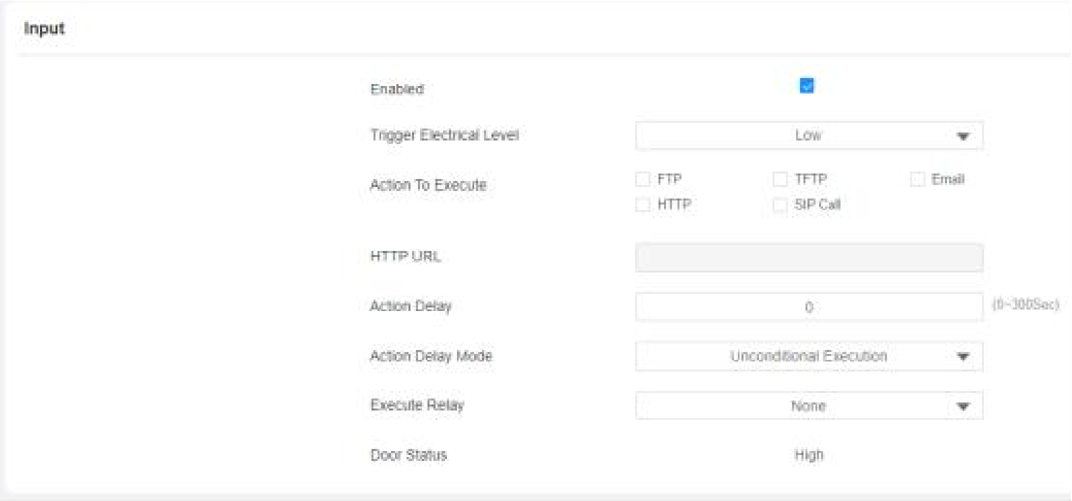
http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

Note

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

11.9 Unlock by Exit Button by the Door

When you need to open the door from inside using the exit button installed by the door, you can configure the access control terminal Input to trigger the relay for the door access. To configure the configuration on web **Access Control > Input > Input** interface.



Input

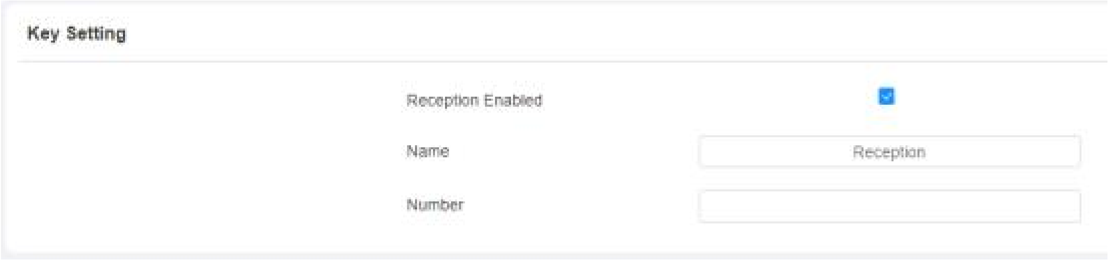
Enabled	☑
Trigger Electrical Level	Low
Action To Execute	□ FTP □ TFTP □ Email □ HTTP □ SIP Call
HTTP URL	
Action Delay	0 (0~300Sec)
Action Delay Mode	Unconditional Execution
Execute Relay	None
Door Status	High

Parameter Set-up:

- **Enabled**: it is enabled by default.
- **Trigger Electrical Level:** select the trigger electrical level options between **High** and **Low** according to the actual operation on the exit button.
- **Action to Execute:** select the method to carry out the action among four options: **FTP, Email, HTTP, and TFTP.**
- **HTTP URL:** enter the URL if you select the HTTP to carry out the action.
- **Action Delay:** set up the delay time when the action is carried out. For example, if you set the action delay time at 5 seconds, then the corresponding actions will be carried out 5 minutes after you press the button(input is triggered).
- **Action Delay Mode:** if you select **Unconditional Execution**, then action will be carried out when the input is triggered. If you select **Execute If Input Still Triggered**, then the action will be carried out if the input stays triggered. For example, if the door stays open after triggering input, an action such as an email will be sent to notify the receiver.
- **Execute Relay:** set up relays to be triggered by the input.
- **Door Status:** display the status of the input signal.

11.10 Unlock by Reception Tab

On the device's home screen, the E16C door phone provides residents and visitors quick door access by pressing the **Reception** tab at the bottom of the home screen. To do the configuration, you can go to **Intercom > Basic > Key Setting.**



Key Setting

Reception Enabled	☑
Name	Reception
Number	

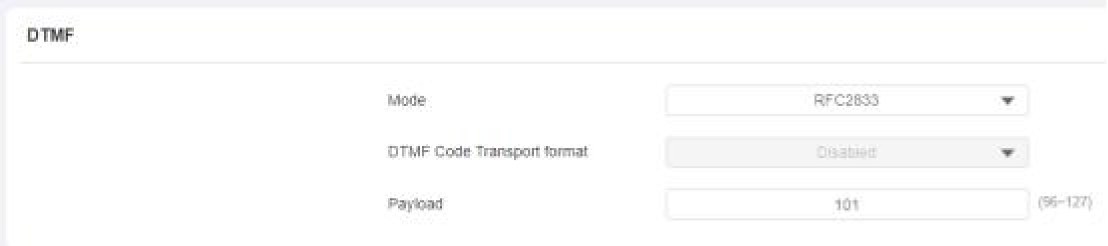
Parameter Set-up:

- **Reception Enabled:** tick the check box to enable the function.

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

11.11 Unlock by DTMF Code

DTMF codes can be configured on the door phone web interface and set up identical DTMF codes on the corresponding intercom devices such as the indoor monitor, which allows residents to enter the DTMF code on the soft keypad or press the DTMF code attached to unlock tab on the screen to unlock the door for visitors etc., during a call. To do the extra DTMF configuration on the web interface, you can go to **Account > Advanced > DTMF** interface**.**



DTMF

Mode	RFC2833 ▾	
DTMF Code Transport format	Disabled ▾	
Payload	101	(96~127)

Parameter Set-up:

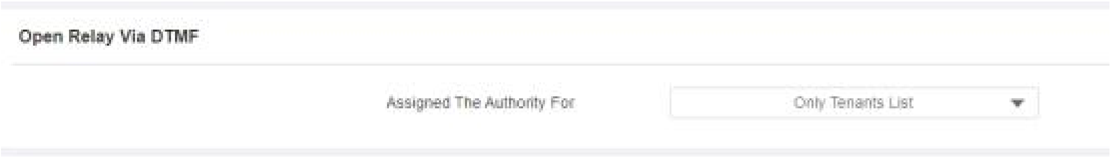
- **Type:** select DTMF type among five options: **Inband, RFC2833, Info+Inband,** and **Info+RFC2833** according to your need.
- **How to Notify DTMF:** select among four options: **Disable, DTMF, DTMF-Relay,** and **Telephone-Event** according to your need.
- **DTMF Payload:** select the payload 96-127 for data transmission identification.

Note

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

11.11.1 Configure DTMF White List

In order to secure the door access via DTMF codes, you can set up the DTMF whitelist on the device web **Access Control > Relay > Open Relay Via DTMF** interface so that only the caller numbers you designated in the door phone can use the DTMF code to gain door access.



Open Relay Via DTMF

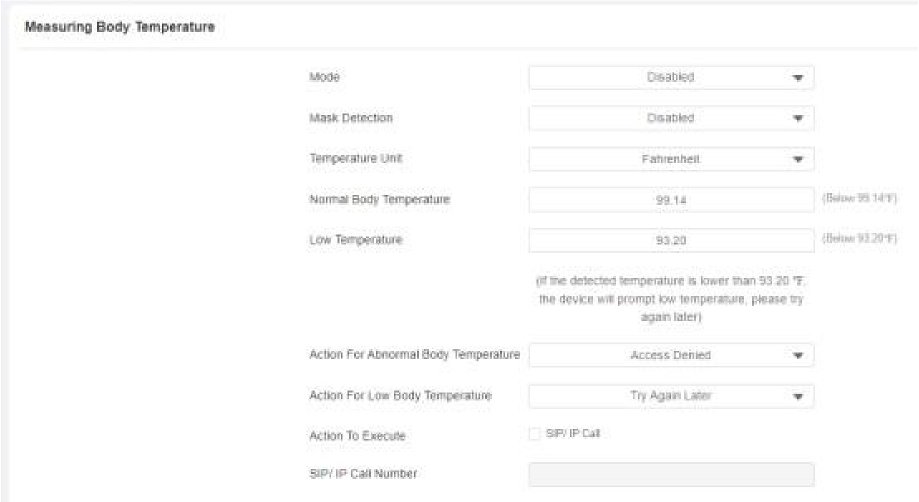
Assigned The Authority For: Only Tenants List

11.12 Body Temperature Measurement for Door Access （Optional）

E16C provides you with an optional body temperature measurement function designed to be applied in the situation where the measurement becomes necessary for the safety of the residents and visitors etc. Residents and visitors are required to go through temperature measurements along with an optional mask detection check before they are allowed for door access.

11.12.1 Body Temperature Measurement Configuration

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



Measuring Body Temperature

Mode	Disabled
Mask Detection	Disabled
Temperature Unit	Fahrenheit
Normal Body Temperature	99.14 (Below 99.14°F)
Low Temperature	93.20 (Below 93.20°F)
	(If the detected temperature is lower than 93.20 °F, 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 or **Wrist** 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. A warning alarm will be triggered when the body temperature measured is detected higher than the defined normal body temperature.
- **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 the temperature is lower than 34 degrees celsius will be deemed as low body temperature.
- **Low Temperature**: set the low temperature.
- **Action For Abnormal Body Temperature:** if you select **Access Denied** then anyone who is detected with abnormal body temperature will be denied the door access. If

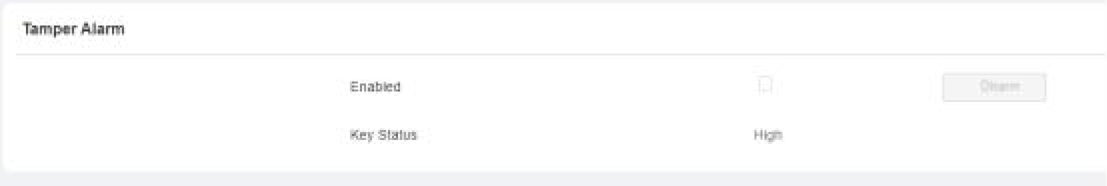
you select **Just For Reminder** then anyone with abnormal body temperature will still be granted the door access.

- **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 the 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 box in the **Action to Execute**.

12 Security

12.1 Tamper Alarm Setting

The tamper alarm function serves as a protection against any unauthorized removal of the device by triggering off the temper alarm on the device. To configure the configuration on web **Security > Basic > Temper Alarm** interface.



Tamper Alarm

Enabled □ Disarm

Key Status High

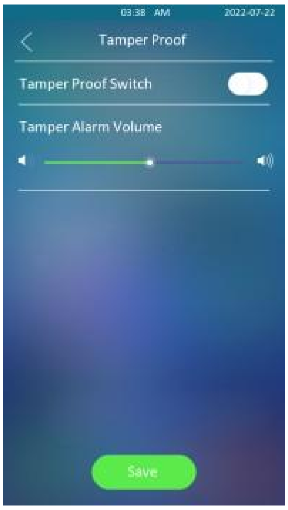
Parameter Set-up:

- **Enable**: tick the check box to enable the temper alarm function. When the temper alarm goes off, you can press the **Disarm** tab beside the check box to clear the alarm.
- **Key Status**: when the tamper alarm button pops up, then the status will be changed from low to high. The normal state is high.

Note

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

To turn on the tamper-proof function on the device, tap **Security > Temper Proof**.



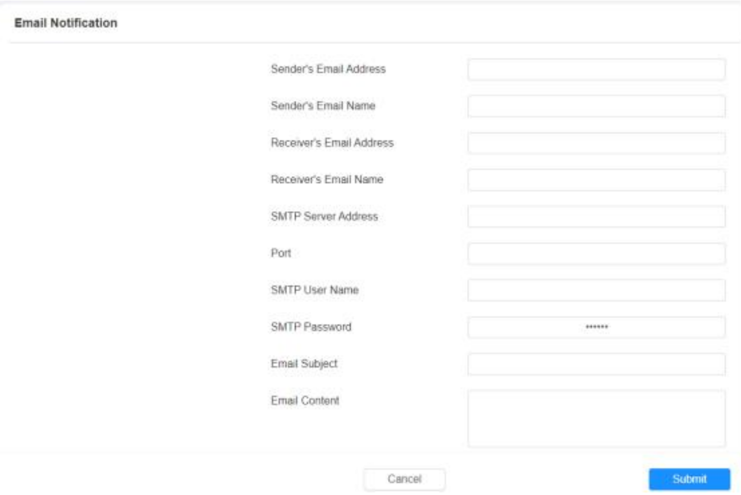
Tamper Proof Switch

Tamper Alarm Volume

12.2 Security Notification Setting

12.2.1 Email Notification Setting

If you want to receive the security notification via email, you can configure the Email notification on the web interface properly. To configure the configuration on web **Setting > Action > Email Notification** interface.



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	

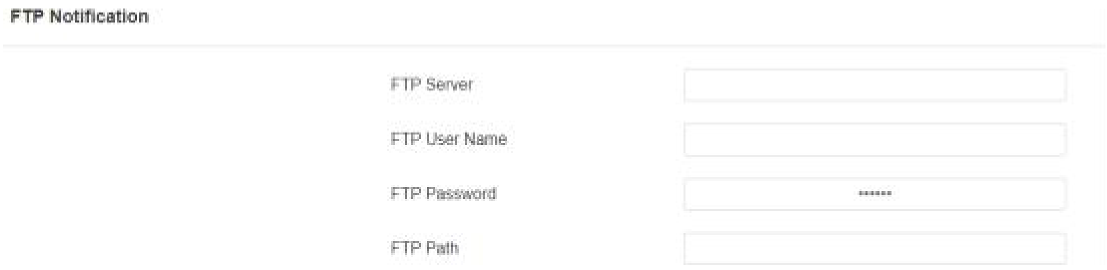
Parameter Set-up:

- **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 as the sender's email address.
- **SMTP Password:** configure the password of the SMTP service, which is the same as the sender's email address.
- **Email Subject:** enter the subject of the email.
- **Email Content:** compile the email contents according to your need.

FTP Notification setting

If you want to receive the security notification via FTP, you can configure the FTP notification on the web interface properly. To configure the configuration on web **Setting > Action > FTP Notification** interface.



FTP Notification

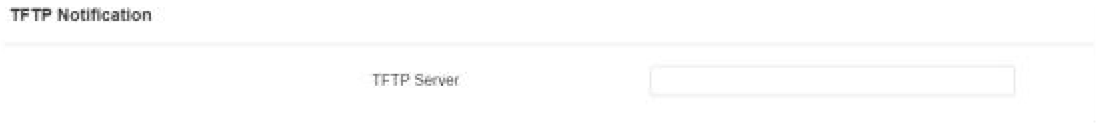
FTP Server	
FTP User Name	
FTP Password	••••••
FTP Path	

Parameter Set-up:

- **FTP server**: enter the address (URL) of the FTP server for the FTP notification.
- **FTP User Name**: enter the FTP server user name.
- **FTP Password**: enter the FTP server password.
- **FTP Path**: enter the folder name you created in the FTP server.

TFTP Notification Setting

If you want to receive the security notification via TFTP, you can configure the FTP notification on the web interface properly. To configure the configuration on web **Setting > Action > TFTP Notification** interface.



TFTP Notification

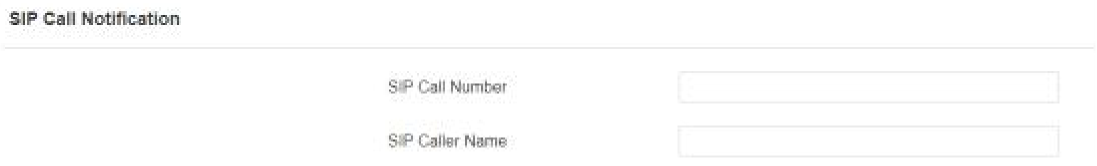
TFTP Server

Parameter set-up:

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

12.2.2 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

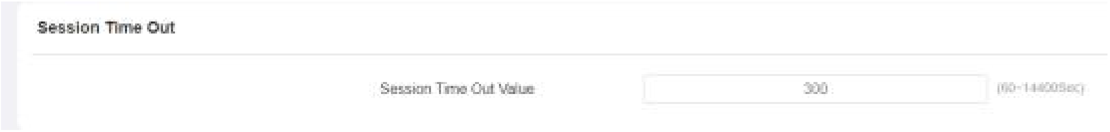
SIP Caller Name

Parameter set-up:

- **SIP Call Number**: enter the SIP call number IP number.
- **SIP Caller Name**: enter the name of the called party.

12.3 Web Interface Automatic Log-out

You can set up the web interface automatic log-out timing, requiring re-login by entering the user name and the passwords for security purposes or for the convenience of operation. To configure the configuration on web **System> Security > Session Time Out** interface.



Session Time Out

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

Parameter Set-up:

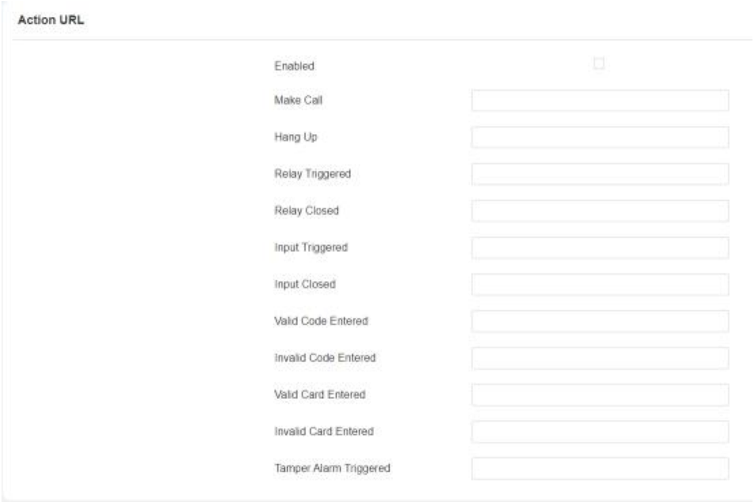
- **Session Time Out Value:** set the automatic web interface logout timing ranging from 60 seconds to 14400 seconds. The default value is 300.
- **TFTP Server**: enter the address (URL) of the TFTP server for the FTP notification.

12.4 Action URL

E16C allows you to set up specific HTTP URL command that will be sent to the HTTP server for the predefined actions. Relevant actions will be initiated if there occur any changes in the relay status, input status, PIN code, and RF card access for security purposes. You can navigate to **Setting > Actions URL**

Note

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



Action URL

Enabled □

Make Call

Hang Up

Relay Triggered

Relay Closed

Input Triggered

Input Closed

Valid Code Entered

Invalid Code Entered

Valid Card Entered

Invalid Card Entered

Tamper Alarm Triggered

For example :

http://192.168.16.118/help.xml?
mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_s n=$card_sn

Akuvox supports the following parameter format for the event below.

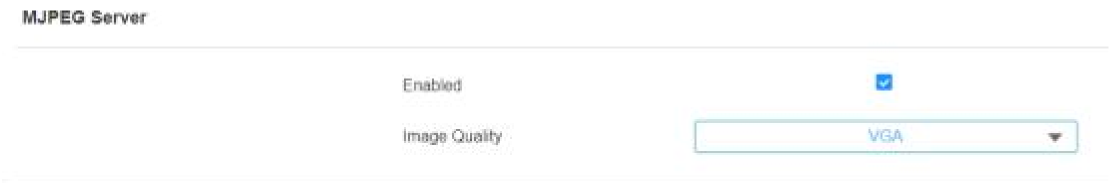
No.	Event	Parameter format	Example
1	Make Call	$remote	Http://server ip/ Callnumber=$remote
2	Hang Up	$remote	Http://server ip/ Callnumber=$remote
3	Relay Triggered	$relay1status	Http://server ip/ relaytrigger=$relay1status
5	Relay Closed	$relay1status	Http://server ip/ relayclose=$relay1status
6	Input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

11	Invalid Car Entered	$card_sn	Http://server ip/ invalidcard=$card_sn
12	Tamper Alarm Triggered	$alarm status	Http://server ip/ tampertrigger=$alarm status

13 Monitor and Image

13.1 MJPEG Image Capturing

E16C allows you to capture the MJPEG format monitoring image if needed. You can enable the MJPEG function and set the image quality on the web interface. To configure the configuration on web **Surveillance > MJPEG > MJPEG Server** interface.



MJPEG Server

Enabled ☑

Image Quality VGA

Parameter Set-up:

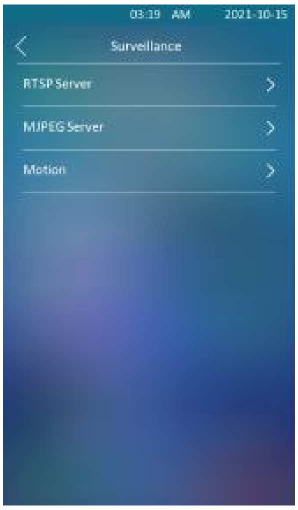
- **Enabled**: tick the check box to enable or disable the Mjpeg service.
- **Image Quality**: select the quality for the image capturing among seven options: **QCIF, QVGA, CIF, VGA, 4CIF, 720P, 1080P**

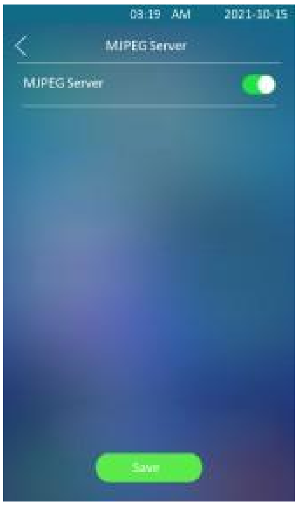
After the MJPEG service is enabled, you can capture the image from the door phone using the following three types of URL format:

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

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

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

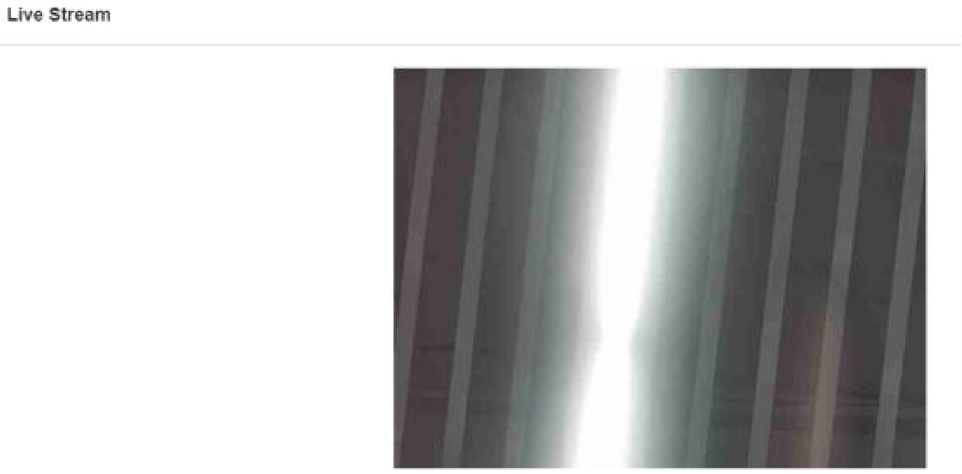




13.2 Live Stream

If you want to check the real-time video from the E16C access control terminal, you can go to the device web interface to obtain the real-time video or you can also enter the correct URL on the web browser to obtain it directly.

To see the live stream on web **Surveillance > Live Stream** interface.



To check the real-time video using a URL, you can Enter the correct URL (**http:// IP_address:8080/video.cgi**).

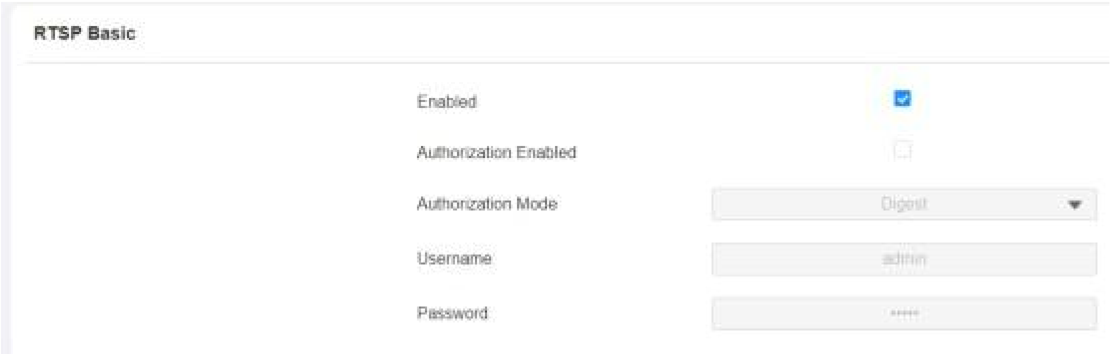
For example http://192.168.2.5:8080/video.cgi

13.3 RTSP Stream Monitoring

E16C door phones support RTSP stream that allows intercom devices such as an indoor monitor or the monitoring unit from the third party to monitor or obtain the real-time audio/ video (RTSP stream) from the door phone using the correct URL.

13.3.1 RTSP Basic Setting

You are required to set up the RTSP function in terms of RTSP Authorization, authentication, password, etc. before you are able to use the function. To configure the configuration on web **Surveillance > RTSP > RTSP Basic** interface.



RTSP Basic

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

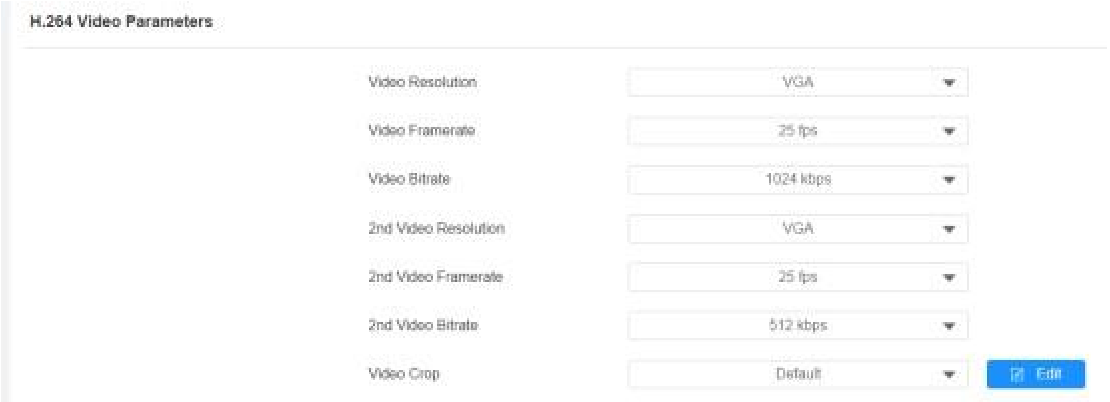
Parameter Set-up:

- **Enabled:** tick the check box to turn on or turn off the RTSP function.

- **AuthorizationEnabled**: 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, and RTSP Password on the intercom device such as an indoor monitor for authorization.
- **Authentication Mode**: select RTSP authentication type between **Basic** and **Digest**. **Basic** is the default authentication type.
- **Username**: enter the name used for RTSP authorization.
- **Password**: enter the password for RTSP authorization.

13.3.2 RTSP Stream Setting

You can select the video codec format for the RTSP stream for the monitoring and you can also configure video resolution and bitrate etc. based on your actual network environment on the web interface. To configure the configuration on web **Surveillance > RTSP > H.264 Video Parameters** interface.



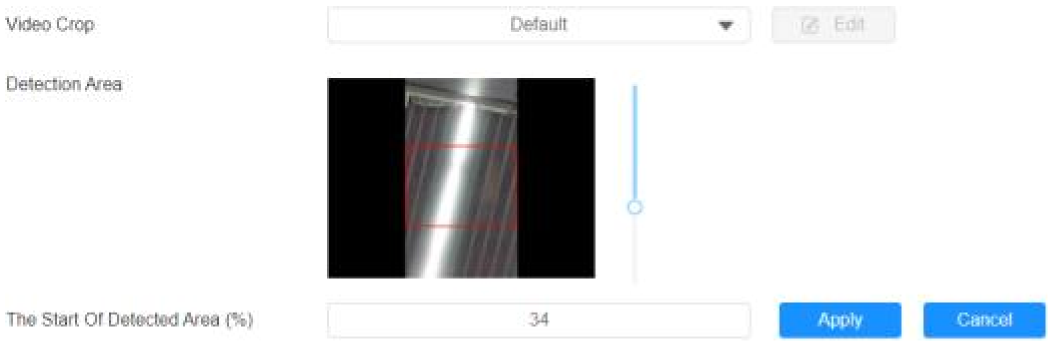
H.264 Video Parameters

Video Resolution	VGA
Video Framerate	25 fps
Video Bitrate	1024 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**, and **1080P**. The default video resolution is **720P**, 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 **720P**.
- **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, and 4096 kbps** according to your network environment. The default video bit rate is **2048 kbps**.
- **2nd Video Resolution2**: select 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 **Original** for the full-screen video display. And select **Default** if you only want to select the specific area on the video to be displayed. You can click **Edit** to start video cropping.



Video Crop: Default

Detection Area

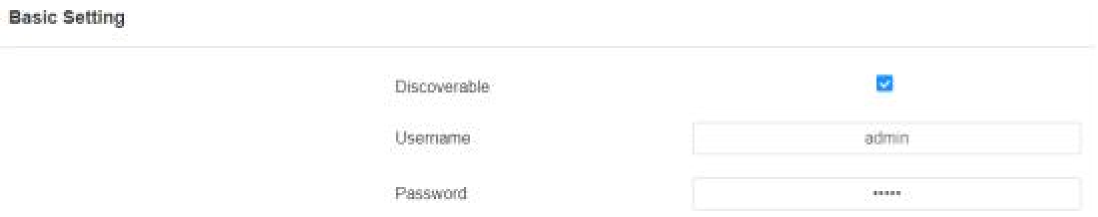
The Start Of Detected Area (%): 34

Note

- E16C supports two video stream channels for H.264 codec video stream.

13.4 ONVIF

Real-time video from the E16C access control terminal camera can be searched and obtained by the Akuvox indoor monitor or by third-party devices such as NVR (**Network Video Recorder**) you can configure the ONVIF function in the access control terminal so that other devices will be able to see the video from the access control terminal. To configure the configuration on web **Surveillance > ONVIF** interface.



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.
- **UserName:** 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.

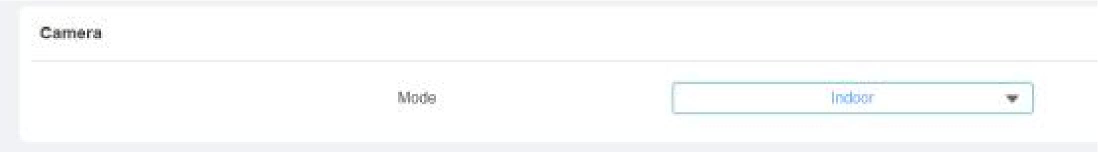
For example: **http://IP address:80/onvif/device_service**

Note

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

13.5 Camera Mode

You can select the camera mode for better video quality depending on where the door phone is located. You can select Indoor mode for better video image(RTSP, ONVIF, and Mjpeg) if the door phone is placed indoors. On the contrary, you can select **Outdoor mode** if the door phone is placed outdoors.



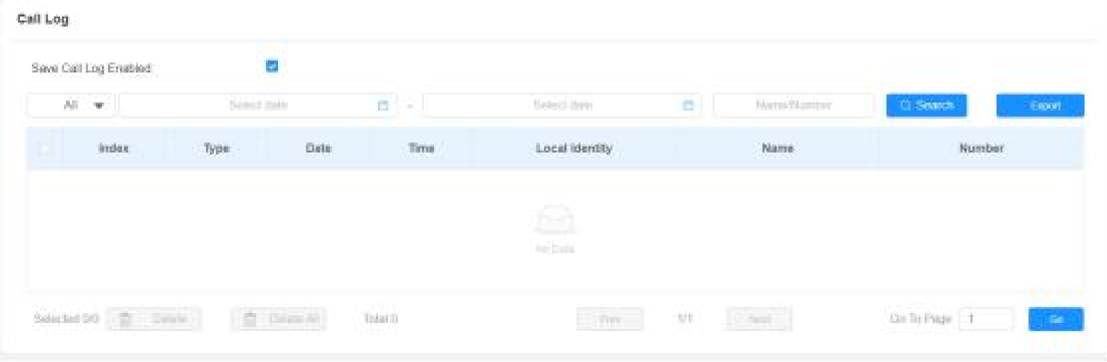
Camera

Mode: Indoor

14 Logs

14.1 Call Logs

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



Call Log

Save Call Log Enabled ☑

	Index	Type	Date	Time	Local Identity	Name	Number

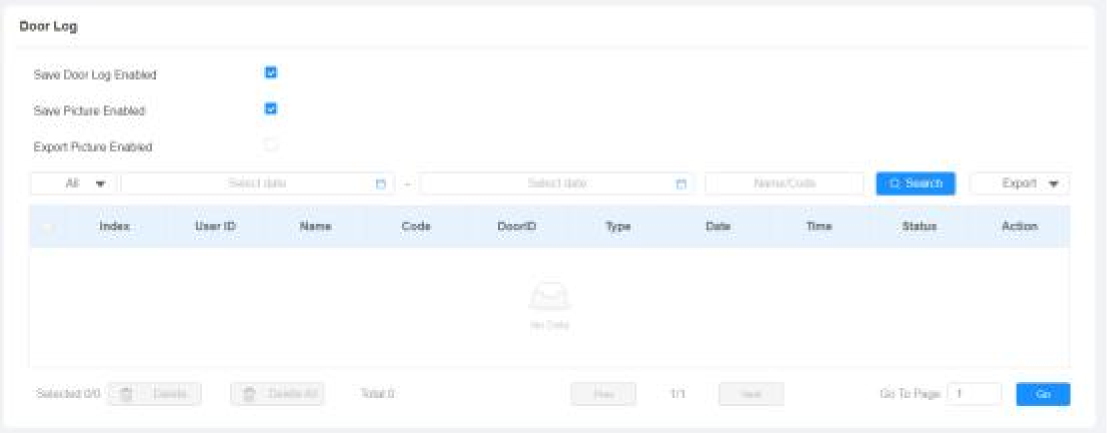
No Data

Parameter Set-up:

- **Save Call Log Enabled**: tick the check box to enable the call log function.
- **Call History**: select call history among four options: **All**, **Dialed**, **Received**, and **Missed** for the specific type of call log to be displayed.
- **Start Time ~ End Time**: select the specific time span of the call logs you want to search, check, or export.
- **Local Identity**: displays the door phone's SIP account or IP number that receives incoming calls.
- **Name/Number**: select the **Name** and **Number** options to search call log by the name or by the SIP or IP number.

14.2 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. To check door logs, go to **Status > Access.**



Door Log

Save Door Log Enabled ☑

Save Picture Enabled ☑

Export Picture Enabled □

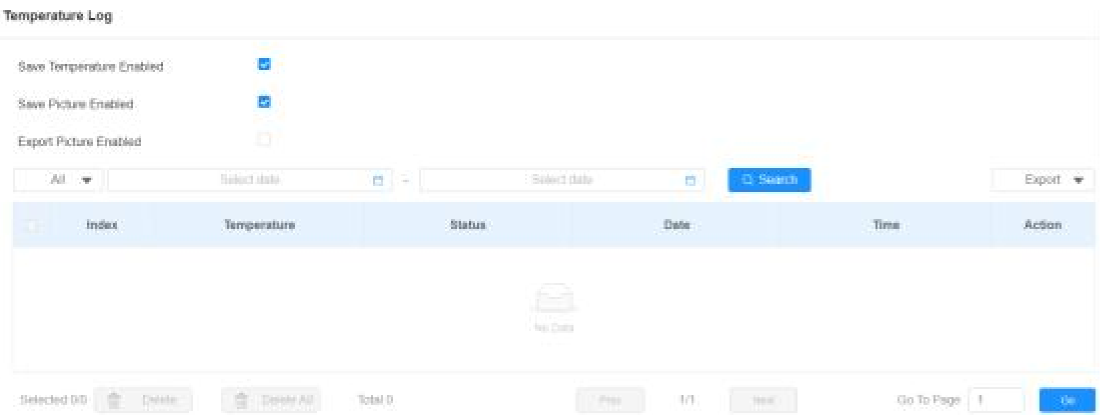
□	Index	User ID	Name	Code	DoorID	Type	Date	Time	Status	Action

Parameter Set-up:

- **Save Door Log Enabled:** tick the check box to turn on or turn off the door log function.
- **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 door log by the name or by the PIN code.
- **Action**: click to display the picture captured.

14.3 Temperature Log

To check the temperature log, go to **Access Control > Temperature Log**.



Temperature Log

Save Temperature Enabled ☑

Save Picture Enabled ☑

Export Picture Enabled □

□	Index	Temperature	Status	Date	Time	Action

No Data

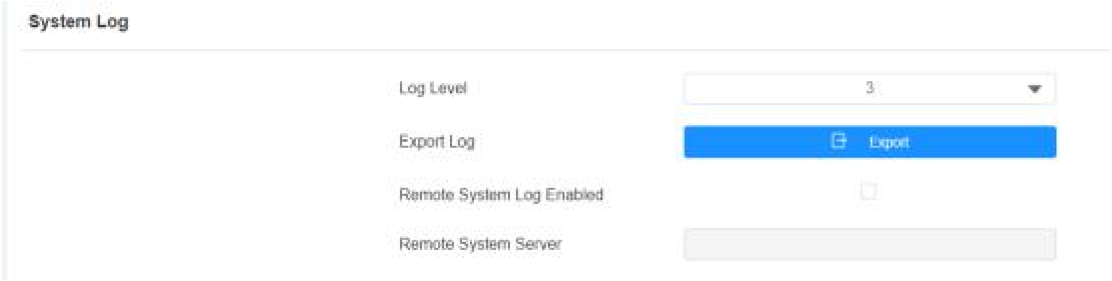
Parameter Set-up:

- **Save Temperature Enabled:** tick the check box to turn on or turn off the temperature Log.
- **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.

15 Debug

15.1 System Log for Debugging

System log in the access control terminal can be used for debugging purposes. If you want to export the system out to a local PC or to a remote server for debugging, you can set up the function on the web **System > Maintenance > System Log interface.**



System Log

Log Level: 3

Export Log: Export

Remote System Log Enabled: □

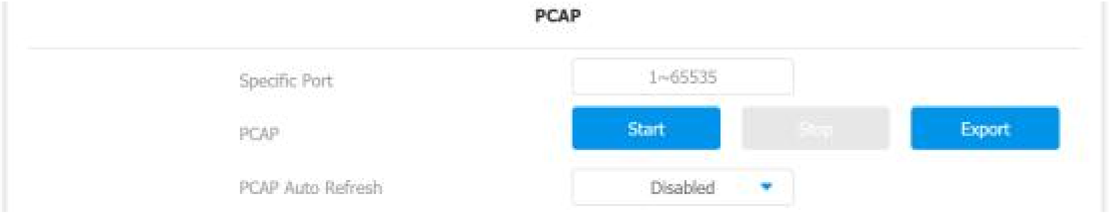
Remote System Server:

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**: go to the **Export** tab to export a temporary debug log file to a local PC.
- **Remote System Log Enabled**: select **Enable** or **Disable** if you want to enable or disable the remote system log.
- **Remote System Server**: enter the remote server address to receive the device log.

15.2 PCAP for Debugging

PCAP is used to capture the data package going in and out of the devices for debugging and troubleshooting purposes. You can set up the PCAP on the device web **System > Maintenance > PCAP** properly before using it.



PCAP

Specific Port: 1~65535

PCAP: Start | Stop | Export

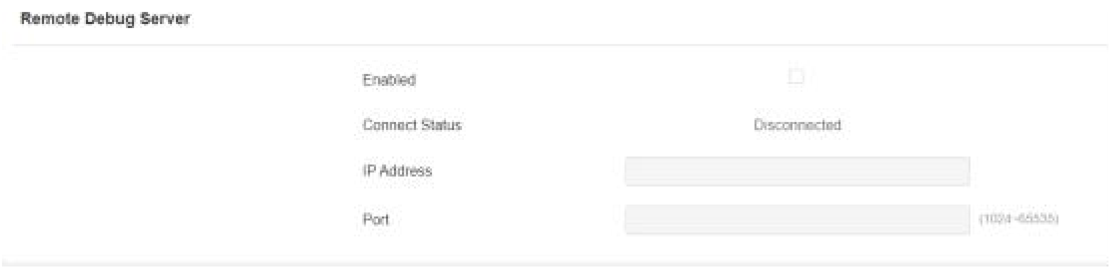
PCAP Auto Refresh: Disabled

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**: go to the start tab and **Stop** tab to capture a certain range of data packets before going to 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.

15.3 Remote Debug Server

You can set up a remote debug server so that Akuvox technical team will be able to obtain the log remotely for debugging. To configure the server, go to **System > Maintenance > Remote Debug Server.**



Remote Debug Server

Enabled: □

Connect Status: Disconnected

IP Address:

Port: (1024~65535)

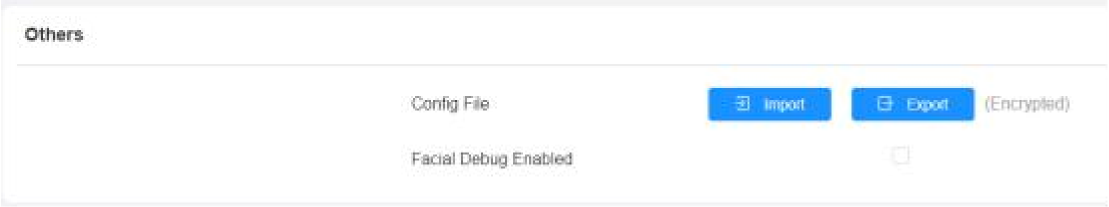
Parameter Set-up:

- **Enabled**: enable the debug server before debugging.
- **Connect Status**: display the remote debug server connection status.

- **IP Address**: enter the remote debug server IP address. Please ask Akuvox technical team for the server IP address.
- **Port**: type in the remote debug server port.

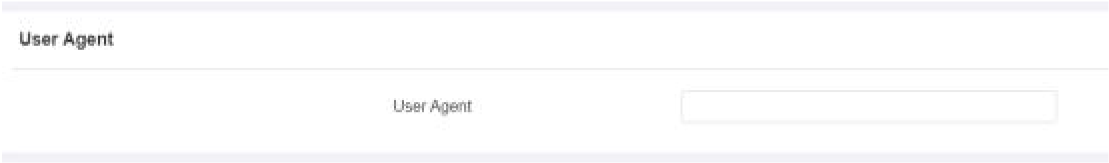
15.4 Face Recognition Debug

You might be required to enable face recognition to debug when you have a face recognition problem. To enable it, go to **System > Maintenance >Others**.



15.5 User Agent

SIP user agent (UA) is an endpoint device that supports SIP, which is used to establish connections and enable sessions between two endpoint devices. And a UA is comprised of UAC (User Agent Client) and UAS (User Agent server) with the UAC used to issue requests and UAS used to issue responses. UA acts as a SIP service provider for the specific user (device). You can customize the user agent field in the SIP message. If the user agent is set to a specific value, users can see the information from PCAP. If a user agent is blank, by default, users can see the company name “Akuvox”, model number, and firmware version from PCAP. Path: **Account > Advanced > User Agent** interface.

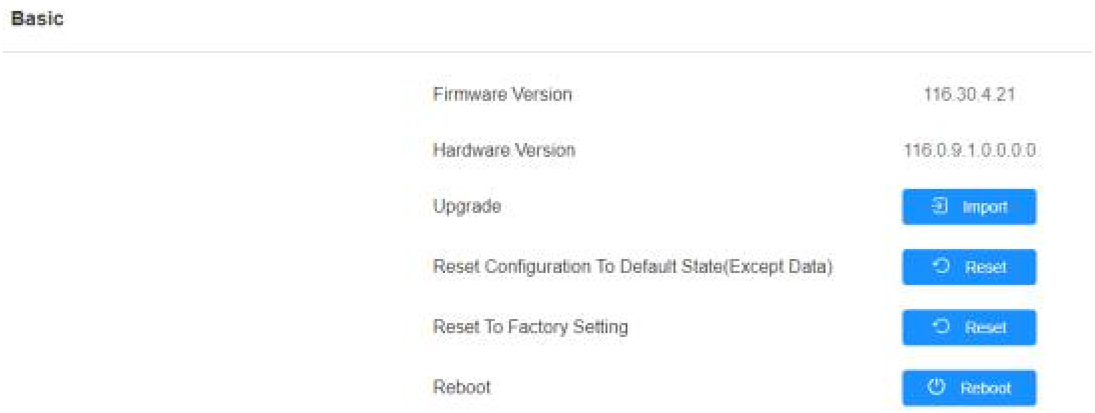


Parameter Set-up:

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

16 Firmware Upgrade

E16C door phones can be upgraded on the device web interface. You can go to **System > Upgrade.**



Basic

Firmware Version 116.30.4.21

Hardware Version 116.0.9.1.0.0.0.0

Upgrade

Reset Configuration To Default State(Except Data)

Reset To Factory Setting

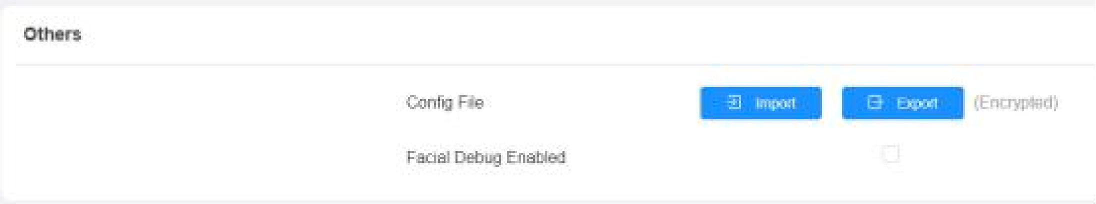
Reboot

Note

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

17 Backup

If you want to import or export encrypted configuration files to your Local PC, go to **System > Maintenance > Others.**



Others

Config File

(Encrypted)

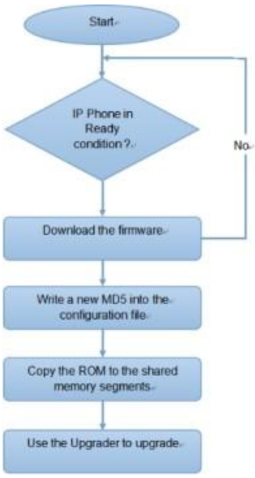
Facial Debug Enabled □

18 Auto-provisioning via Configuration File

Configurations and upgrading on the E16C door phone 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 door phone.

18.1 Provisioning Principle

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


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

18.2 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 another one is the MAC-based configuration provisioning.

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

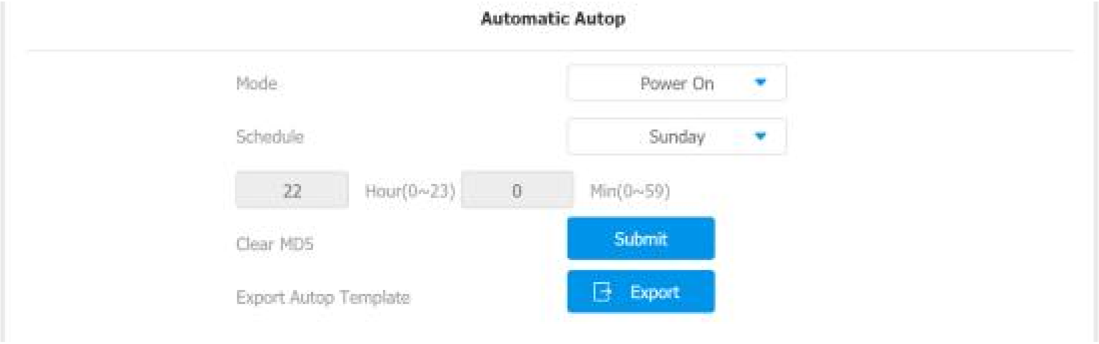
- **General configuration provisioning**: a general file is stored in a server from which all the related devices will be able to download the same configuration file to update parameters on the devices. For example, cfg.
- **MAC-based configuration provisioning**: MAC-based configuration files are used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

Note

- If a server has these two types of configuration files, then IP devices will first access the general configuration files before accessing the MAC-based configuration files.

18.3 AutoP Schedule

Akuvox provides you with different AutoP methods that enable the door phone to perform provisioning for itself at a specific time according to your schedule. You can go **to System > Auto Provisioning.**



Automatic Autop

Mode: Power On

Schedule: Sunday

22 Hour(0~23) 0 Min(0~59)

Clear MD5: Submit

Export Autop Template: Export

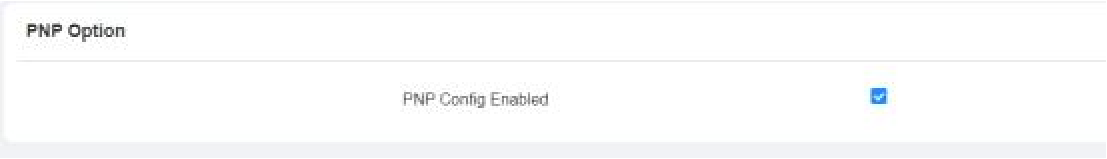
Parameter Set-up:

- **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 setup.
- **Hourly Repeat:** select **Hourly Repeat** if you want the device to perform Autop every hour.

18.4 PNP Configuration

Plug and Play (PNP) is a combination of hardware and software support that enables a computer system to recognize and adapt to hardware configuration changes with little or no intervention by a user. To configure the configuration on the web **System > Auto Provisioning > PNP Option** interface.

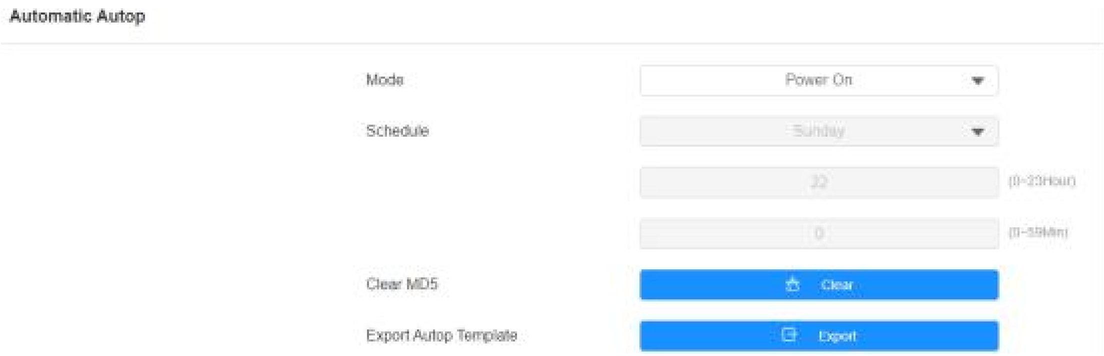


PNP Option

PNP Config Enabled ☑

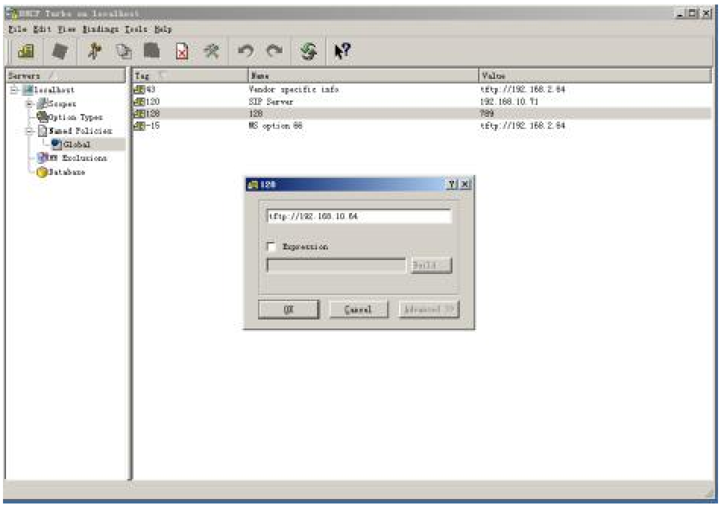
18.5 DHCP Provisioning Configuration

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 code ranging from 128-255), you are required to configure DHCP Custom Option on the web interface. To set up DHCP AutoP with “Custom Option” and “Power on” mode, on web **System > Auto Provisioning > Automatic Autop** interface. Click **Export** tab in **Export Autop Template** to export Autop template. Then set up DHCP Option on DHCP server.



Automatic Autop

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



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

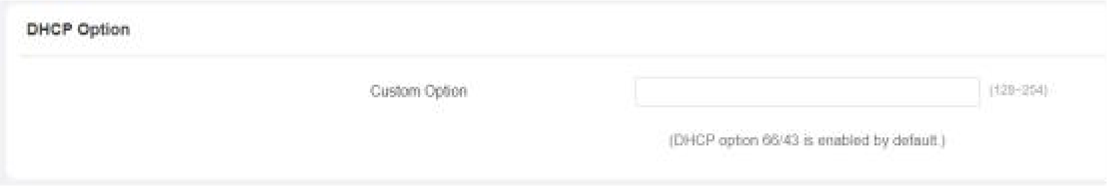
128

tftp://192.168.10.64

☐ Expression

Note

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



DHCP Option

Custom Option (128~254)

(DHCP option 66/43 is enabled by default.)

Parameter Set-up:

- **Custom Option**: enter the DHCP code that matched the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.

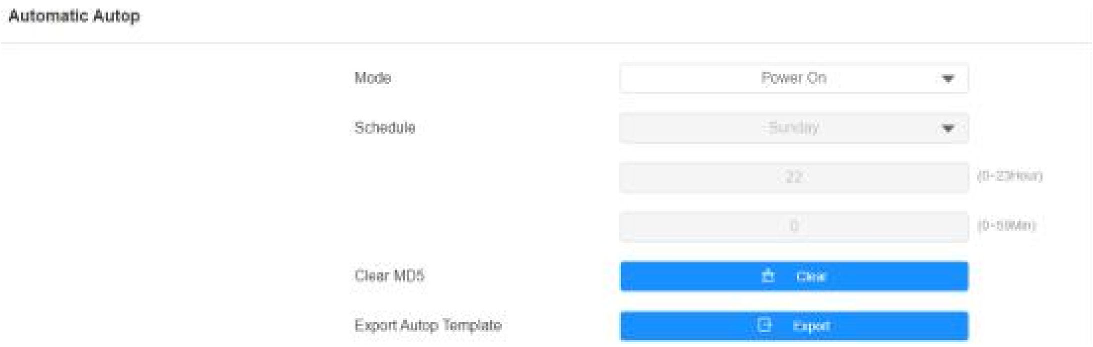
- **DHCP Option 66:** if none of the above is set, the device will automatically use DHCP Option 66 for getting the upgrade server URL. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 66 with the updated server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

Note

- The general configuration file for the in-batch provisioning is with the format **rcfg** taking E16C as an example r000000000116.cfg (9 zero 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,

18.6 Static Provisioning Configuration

You can manually set up a specific server URL for downloading the firmware or configuration file. If an autop schedule is set up, the door phone will perform the auto-provisioning on a specific timing according to autop 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

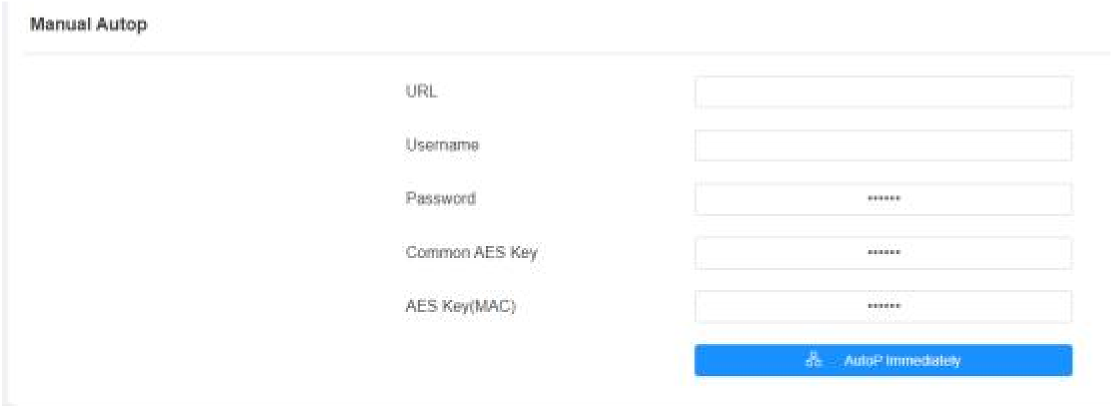
Schedule: Sunday

22 (0-23Hour)

0 (0-59Min)

Clear MD5

Export Autop Template



Manual Autop

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

Parameter Set-up:

- **URL**: set up TFTP, HTTP, HTTPS, and FTP server addresses for the provisioning.
- **User Name**: set up a user name if the server needs a user name to be accessed otherwise leave it.
- **Password**: set up a password if the server needs the password to be accessed otherwise leave it.
- **Common AES Key**: set upAES code for the intercom to decipher the general Auto Provisioning configuration files.

- **AES Key (MAC)**: set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

Note

- AES is one type of encryption, it should be configured only when the config file is encrypted with AES, otherwise leave the field blank.

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)

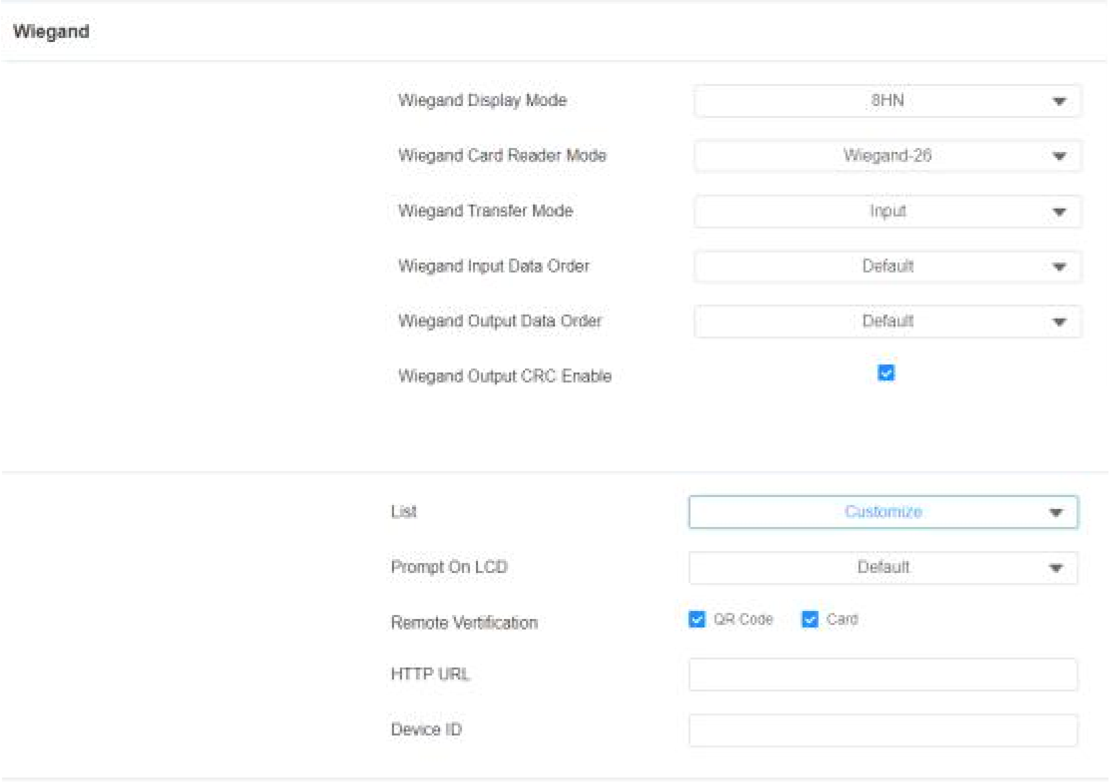
Note

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

19 Integration with Third Party Device

19.1 Integration via Wiegand

If you want to integrate the E16C door phone with the third-party devices via Wiegand. To configure it, you can go to the web **Device > Wiegand** interface.



Wiegand

Wiegand Display Mode: 8HN

Wiegand Card Reader Mode: Wiegand-26

Wiegand Transfer Mode: Input

Wiegand Input Data Order: Default

Wiegand Output Data Order: Default

Wiegand Output CRC Enable: ☑

List: Customize

Prompt On LCD: Default

Remote Verification: ☑ QR Code ☑ Card

HTTP URL:

Device ID:

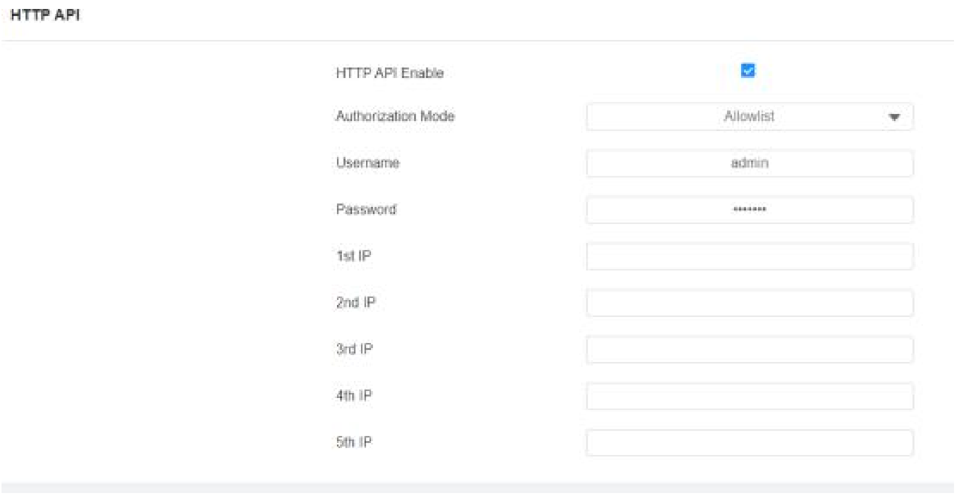
Parameter Set-up:

- **Wiegand Display Mode:** select Wigand Card code format among **8H10D; 6H3D5D; 6H8D; 8HN; 8HR.**
- **Wiegand Card Reader Mode:** set the Wiegand data transmission format among three options: **Wiegand 26**, **Wiegand 34**, **Wiegand 58**. The transmission format should be identical between the door phone and the device to be integrated.
- **Wiegand Transfer Mode:** set the Transfer mode between **Input** or **Output** if the door phone is used as a receiver, then set it as **Input** for the door phone and vice versa.

- **Wiegand Input Data Order:** set the Wiegand input data sequence between **Normal** and **Reversed** if you select **Reversed** then the input card number will be reversed and vice versa**.**
- **Wiegand Output Basic Data Order:** select **Normal** if you want Wiegand output data to be displayed in a normal state. Select **Reversed** if you want to reverse the output data, for example from "0x110x220x330x44" to "0x440x330x220x11".
- **Wiegand Output Data Order:** set the Wiegand output data sequence between **Normal and Reversed** if you select **Reversed** then the input card number will be reversed and vice versa**.**
- **Wiegand Output CRC:** this function is used for Wiegand data inspection. It is turned on by default. If it is not turned on, you might not be able to integrate the device with third-party devices.

19.2 Integration via HTTP API

HTTP API is designed to achieve a network-based integration between the third-party device with the Akuvox intercom device. You can configure the HTTP API function on the web **Setting > HTTP API** interface for the integration.



HTTP API

HTTP API Enable ☑

Authorization Mode: Allowlist

Username: admin

Password: *******

1st IP

2nd IP

3rd IP

4th IP

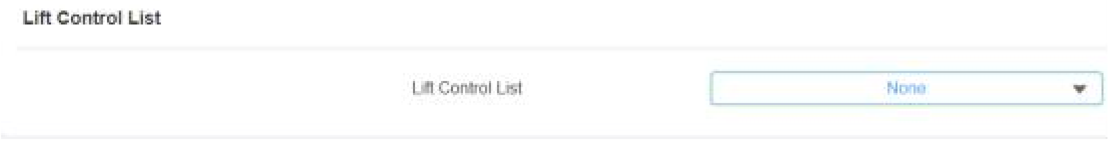
5th IP

Parameter Set-up:

- **HTTP API Enable:** HTTP API Enables or disables 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 HTTP 403 forbidden status will be returned.
- **Authorization Mode:** select among four options**: None, WhiteList, Basic, and Digest** 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.
- **1stIP- 5th IP:** enter the IP address of the third-party devices when the WhiteList authorization is selected for the integration.

19.3 Lift Control

You can connect the E16C door phone with AKuvox EC32 lift controller and third-party lift controllers for the lift control. You can summon the lift to go down to the ground floor when you are granted through various types of access methods on the door phone. To set up the lift control, go to **Device > Lift Control**.



Lift Control List

Lift Control List: None

Parameter Set-up:

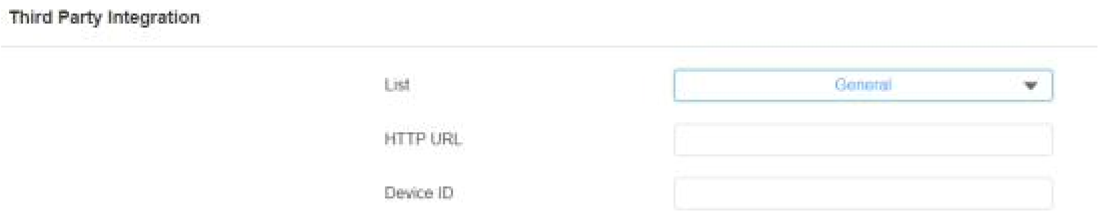
- **Lift Control List**: select integration mode among seven Options: **None, OSDP, Akuvox EC32, KEYKING.** The detail for the options will be provided in the following chart.

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 R29 series 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.

19.4 Integrate with third-party Access Control Server

You can access the door phone using the QR code or access card generated by a third-party server. For example, when you use the QR code on the door phone, the QR code will be sent to the third-party server for verification. And you will be granted access if the QR code passes the verification. To configure it, you can go to **Access Control > Relay > Third Party Integration**.



Third Party Integration

List: General

HTTP URL

Device ID

Parameter Set-up:

- **List**: select the integration modes.
  - If you want to disable the function, select **None**.
  - If you want to use QR code only, select **General**.

- If you want to select between a QR code and an access card with customized features, select **Customize**.

- **HTTP URL:**
  - For General mode: enter the HTTP command format provided by the third-party service provider. After scanning the QR code, the HTTP command will carry the dynamic QR code information automatically before its being sent to the QR code server for verification. See the example below: http:// wxqapi.kerryprops.com.cn:8090/api/vistor/scan?codeKey={QRCode} &deviceId={DeviceID}
  - For Customize mode: select the QR code or Card verification.
  - For QR code verification: enter the QR code HTTP command provided by the third-party service provider. See the example below: /hs/ACS/checking/QR" >http://www.server.com/<base>/hs/ACS/checking/QRCode/{DeviceID}/{Card}
  - For Card verification: enter the access card HTTP command, provided by the third-party service provider. See the example below: http://www.server.com/<base>/hs/ACS/checking/{QRCode}/{DeviceID}/Card

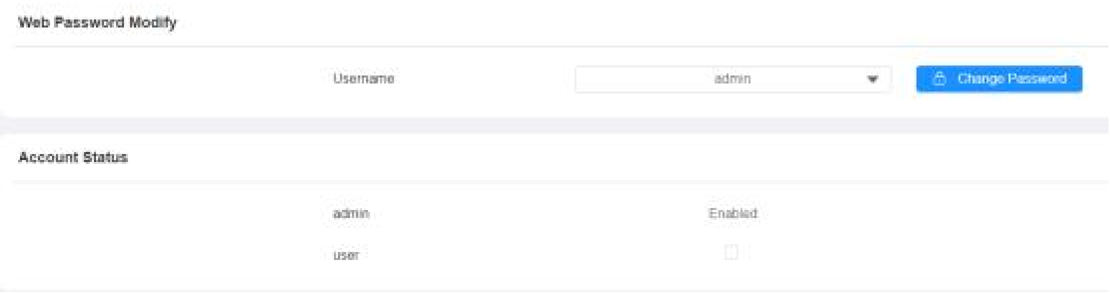
- **Prompt On LCD**: select **Default**, if you want to adopt the Akuvox door phone prompt for the door access. Select **Return** value, if you want to use the return value from the third-party server as the prompt.

- **Remote Verification**: select **QR code** or **Card** verification.

- **Device ID**: enter your device ID, which will be added to the HTTP command automatically when you use a QR code or card for access.

20 Password Modification

You can set and change both the System PIN Code for accessing the device setting and the login password for accessing the web interface. In addition, you can also select the user role when setting passwords. To set the password, go to **System > Security > Web Password Modify**



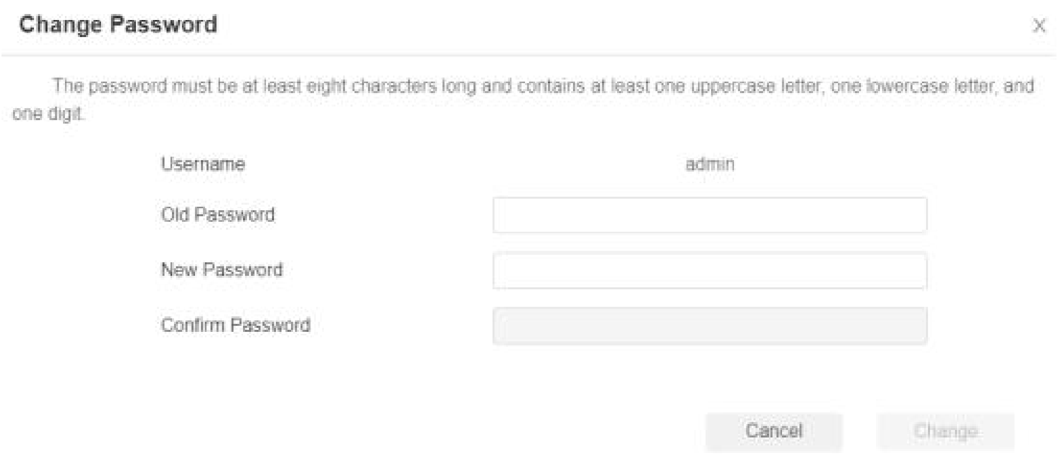
Web Password Modify

Username: admin

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.

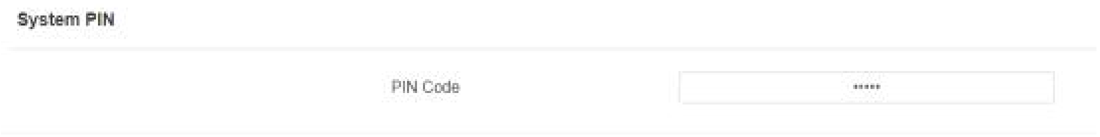
Username: admin

Old Password

New Password

Confirm Password

To set up the system PIN code, you can go to the **system PIN** section.



System PIN

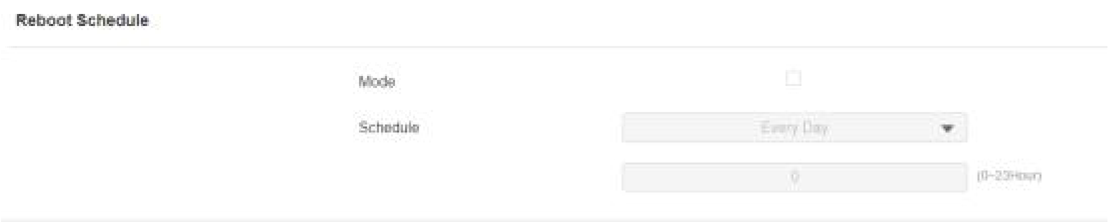
PIN Code: *****

21 System Reboot&Reset

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

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



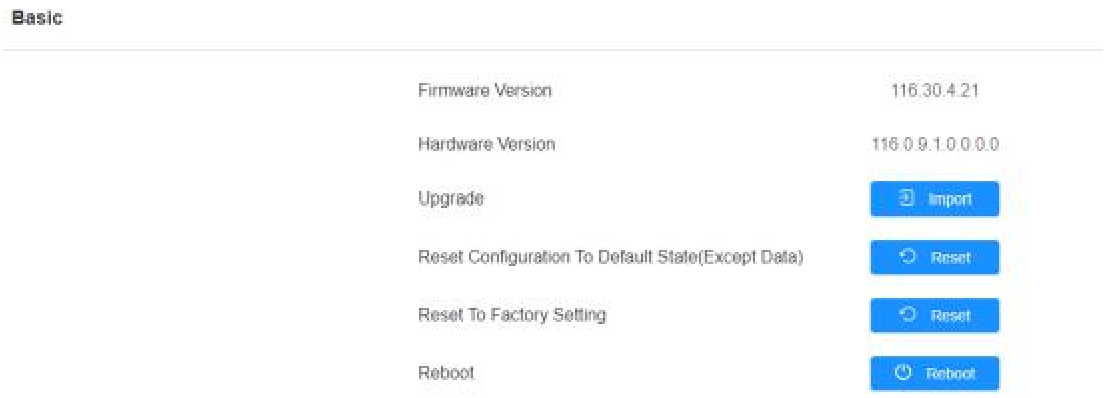
Reboot Schedule

Mode □

Schedule Every Day

0 (0~23Hour)

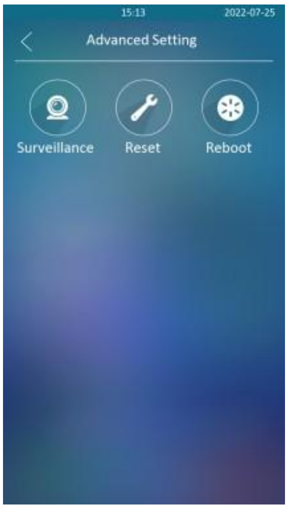
To reboot the device manually, go to **System > Upgrade > Basic**.



Basic

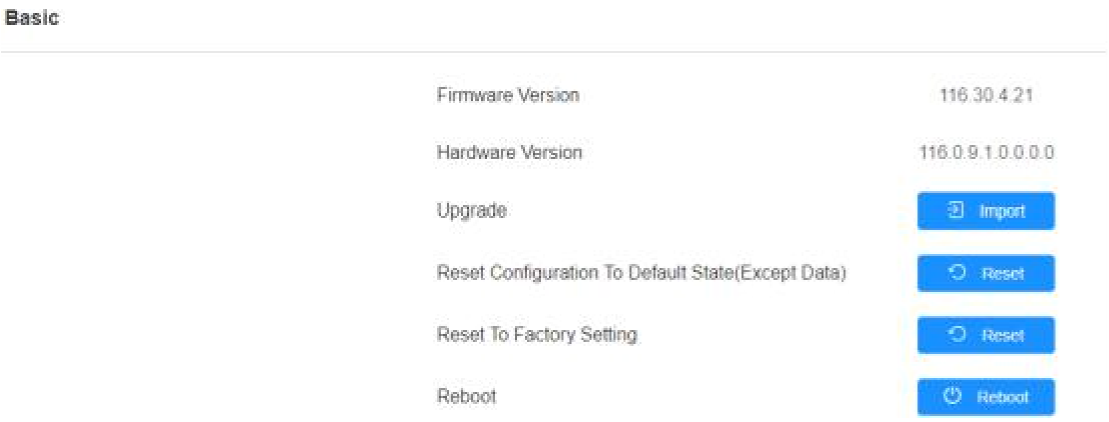
Firmware Version	116.30.4.21
Hardware Version	116.0.9.1.0.0.0.0
Upgrade	Import
Reset Configuration To Default State(Except Data)	Reset
Reset To Factory Setting	Reset
Reboot	Reboot

To reboot the device, tap **Advanced > Reboot**.



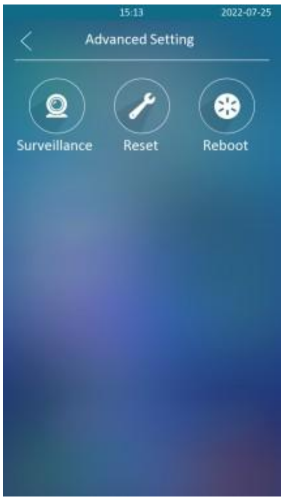
21.2 Reset

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


Basic

Firmware Version	116.30.4.21
Hardware Version	116.0.9.1.0.0.0.0
Upgrade	Import
Reset Configuration To Default State(Except Data)	Reset
Reset To Factory Setting	Reset
Reboot	Reboot

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


15:13
2022-07-25
Advanced Setting
Surveillance
Reset
Reboot

22 Abbreviations

ACS: Auto Configuration Server

Auto: Automatically

AEC: Configurable Acoustic and Line Echo Cancelers

ACD: Automatic Call Distribution

Autop: Automatical Provisioning

AES: Advanced Encryption Standard

BLF: Busy Lamp Field

COM: Common

CPE: Customer Premise Equipment

CWMP: CPE WAN Management Protocol

DTMF: Dual Tone Multi-Frequency

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

DND: Do Not Disturb

DNS-SRV: Service record in the Domain Name System

FTP: File Transfer Protocol

GND: Ground

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure Socket Layer

IP: Internet Protocol

ID: Identification

IR: Infrared

LCD: Liquid Crystal Display

LED: Light Emitting Diode

MAX: Maximum

POE: Power Over Ethernet

PCMA: Pulse Code Mod

PCMA: Pulse Code Modulation A-Law

PCMU: Pulse Code Modulation µ-Law

PCAP: Packet Capture

PNP: Plug and Play

RFID: Radio Frequency Identification

RTP: Real-time Transport Protocol

RTSP: Real Time Streaming Protocol

MPEG: Moving Picture Experts Group

MWI: Message Waiting Indicator

NO: Normal Opened

NC: Normal Connected

NTP: Network Time Protocol

NAT: Network Address Translation

NVR: Network Video Recorder

ONVIF: Open Network Video Interface Forum

SIP: Session Initiation Protocol

SNMP: Simple Network Management Protocol

STUN: Session Traversal Utilities for NAT

SNMP: Simple Mail Transfer Protocol

SDMC: SIP Devices Management Center

TR069: Technical Report069

TCP: Transmission ControlProtocol

TLS: Transport Layer Security

TFTP: Trivial File Transfer Protocol

UDP: User Datagram Protocol

URL: Uniform Resource Locator

VLAN: Virtual Local Area Network

WG: Wiegand

23 Contact Us

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

Sales email: sales@akuvox.com

Technical support email: support@akuvox.com

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

We highly appreciate your feedback about our products.