



AKUVOX E18C DOOR PHONE Administrator Guide

About This Manual

Thank you for choosing Akuvox E18C door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to 18.30.0.54 version, and it provides all the configurations for the functions and features of E18C door phones. Please visit Akuvox forum or consult technical support for any new information or the latest firmwares.

Introduction of Icons and Symbols



Warning:

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



Caution:

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



Note:

- Informative information and advice from the efficient use of the device.



Tip:

- Useful information for the quick and 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>

Table of Contents

1. Product Overview	1
2. Change Log	2
3. Model Specification	3
4. Introduction to Configuration Menu	5
5. Access the Device	7
5.1. Access the Device Setting on the device.....	7
5.2. Access the Device Setting on the Web Interface.....	8
6. Time and Language Setting	10
6.1. Language Setting.....	10
6.1.1. Language Setting on the Device.....	10
6.1.2. Language Setting on the Device Web Interface.....	11
6.2. Time Setting.....	11
6.2.1. Configure Time Setting on the Device.....	11
6.2.2. Time Setting on the Device Web Interface.....	13
6.3. LED Setting.....	14
6.3.1. Configure Card Reader LED Setting.....	14
6.3.2. Configure LED White Light Setting.....	15
6.4. LCD Screen Brightness Setting.....	16
6.4.1. LCD Screen Brightness Setting on the Device.....	16
6.4.2. LCD Screen Brightness Setting on the Web Interface.....	16
6.5. Screen Display configuration.....	17
6.5.1. Configure Screensaver.....	17
6.5.2. Configure Screensaver on the Device.....	17
6.5.3. Configure Screensaver on the Web Interface.....	18
6.5.4. Customize Screensaver on the Web Interface.....	19
6.5.5. Home Screen Configuration.....	20
6.6. Volume & Tone Configuration.....	21
6.6.1. Volume Configuration.....	21
6.6.1.1. Configure Volume on the Device.....	21
6.6.1.2. Configure Volume on the Web Interface.....	22
6.6.2. Upload Open Door Tone.....	23
6.6.3. Configure Door Open Prompt Text.....	23
6.6.4. Configure Hang-up Tone.....	24
7. Network Setting	25
7.1. Device Network Connection Setting.....	25
7.2. LTE Wireless Connection Setting.....	26
7.3. Device Local RTP configuration.....	27
7.4. Device Deployment in Network.....	28
7.5. NAT Setting.....	29

8. Intercom Call Configuration.....	31
8.1. IP call & IP Call Configuration.....	31
8.1.1. Make IP/SIP calls.....	31
8.1.2. IP Call Configuration.....	32
8.2. SIP Call &SIP Call Configuration.....	32
8.2.1. SIP Account Registration.....	33
8.2.1.1. Configure SIP Account on the Device.....	33
8.2.1.2. Configure SIP Account on the Web Interface.....	34
8.2.2. SIP Server Configuration.....	35
8.2.3. Configure SIP Ports for SIP Calls.....	36
8.2.4. Configure Outbound Proxy Server.....	36
8.2.5. Configure Data Transmission Type.....	37
8.3. Dial Options Configuration.....	38
8.3.1. Quick Dial by Number Replacement.....	38
8.3.2. Quick Dial By Number Replacement on the Device.....	38
8.3.2.1. Quick Dial by Number Replacement on the Device.....	39
8.4. Call Auto-answer Configuration.....	40
8.5. Call Settings.....	41
8.5.1. Maximum Call Duration Setting.....	41
8.5.2. Maximum Dial Duration Setting.....	42
8.5.3. Audio& Video Codec Configuration for SIP Calls.....	43
8.5.3.1. Configure Audio Codec.....	43
8.5.3.2. Configure Video Codec.....	44
8.6. Configure DTMF Data Transmission.....	45
9. Phone Book Configuration.....	47
9.1. Phone Book Configuration on the Device.....	47
9.2. Phone Book Configuration on the Web Interface.....	48
9.2.1. Manage Contact Groups on the Web Interface.....	48
9.2.2. Contact List Configuration on the Web Interface.....	48
9.2.2.1. Contact List Display Setting.....	48
10. Relay Switch Setting.....	50
10.1. Relay Switch Setting.....	50
10.2. DTMF Code Configuration.....	51
10.3. Web Relay Setting.....	52
10.3.1. Configure Web Relay on the Web Interface.....	52
10.3.2. Configure Web Relay on the Device.....	54
10.4. Relay Schedule.....	54
11. Door Access Schedule Management.....	56
11.1. Configure Door Access Schedule.....	56
11.1.1. Create Door Access Schedule on the Web Interface.....	56
11.1.2. Create Door Access Schedule on the Device.....	58
11.1.3. Import and Export Door Access Schedule.....	59
11.1.4. Edit the Door Access Schedule.....	60
11.1.4.1. Edit the Door Access Schedule on the Web Interface.....	60

11.1.4.2. Edit the Door Access Schedule on the Device.....	60
12. Door Unlock Configuration.....	62
12.1. Configure PIN Code for Door Unlock.....	62
12.1.1. Configure Public PIN code.....	62
12.1.2. Configure Private PIN Code on the Device.....	63
12.1.3. Configure Private PIN Code on the Web Interface.....	64
12.1.4. Configure Private PIN Access Mode.....	66
12.2. Configure RF Card for Door Unlock.....	66
12.2.1. Configure RF Card on the Web Interface.....	66
12.2.1.1. Configure RF Card Code Format.....	67
12.2.2. Configure Facial Recognition for Door Unlock.....	68
12.2.2.1. Configure Facial Recognition on the Device.....	68
12.2.2.2. Configure Facial Recognition on Web Interface.....	69
12.3. Configure Door Access Using Configured Files.....	69
12.4. Edit the User(s)-specific door access data.....	70
12.4.1. Unlock by QR Code.....	71
12.4.2. Unlock by Bluetooth.....	71
12.4.3. Unlock by NFC.....	72
12.4.4. Unlock by HTTP Command on Web Browser.....	72
12.4.5. Unlock by Exit Button by the Door.....	73
12.4.6. Unlock by Reception Tab.....	74
12.4.7. Body Temperature Measurement for Door Access.....	75
12.4.7.1. Body Temperature Measurement Configuration.....	75
13. Security.....	78
13.1. Tamper Alarm Setting.....	78
13.2. Voice Encryption.....	79
13.3. Motion Detection.....	79
13.3.1. Configure Motion Detection on the Web Interface.....	79
13.3.2. Configure Motion Detection on the Device.....	81
13.4. Security Notification Setting.....	81
13.4.1. Email Notification Setting.....	81
13.4.2. FTP Notification setting.....	83
13.4.3. TFTP Notification Setting.....	83
13.4.4. SIP Call Notification.....	84
13.5. Web Interface Automatic Log-out.....	84
14. Monitor and Image.....	86
14.1. Mjpeg Image Capturing.....	86
14.2. Live Stream.....	87
14.3. RTSP Stream Monitoring.....	89
14.3.1. RTSP Basic Setting.....	89
14.3.2. RTSP Stream Setting.....	90
14.4. ONVIF.....	92
15. Logs.....	94
15.1. Call Logs.....	94

15.2. Door Logs.....	94
15.3. Temperature Log.....	96
15.4. Export Logs.....	96
16. Debug.....	98
16.1. System Log for Debugging.....	98
16.2. PCAP for Debugging.....	99
16.3. User Agent.....	99
17. Firmware Upgrade.....	101
18. Backup.....	103
19. Auto-provisioning.....	105
19.1. Configuration Files for Auto-provisioning.....	105
19.2. AutoP Schedule.....	106
19.3. PNP Configuration.....	106
19.4. DHCP Provisioning Configuration.....	107
19.5. Static Provisioning Configuration.....	108
20. Integration with Third Party Device.....	111
20.1. Integration via Wiegand.....	111
20.2. Integration via RS485.....	112
20.3. OSDP Setting.....	113
20.4. Integration via HTTP API.....	113
20.5. Power Output Control.....	116
21. Password Modification.....	117
22. System Reboot&Reset.....	118
22.1. Reboot.....	118
22.2. Reset.....	119
23. Abbreviations.....	121
24. FAQ.....	123
25. Contact Us.....	126

1. Product Overview

Akuvox E18C is an Linux-based with a touch screen. It incorporates audio and video communications, access control, and video surveillance. Its finely-tuned SmartPlus and AI-based communication technology allow featured customization to better suit your operation habit. E18C multiple ports, such as RS485 and Wiegand ports, can be used to easily integrate external digital systems, such as elevator controller and fire alarm detector, helping to create a holistic control of building entrance and its surroundings and giving you a great sense of security via a variety of access such as card access, NFC, Bluetooth, QR code and newly added door access in an accompaniment with body temperature measurement. E18C door phone applies to residential buildings, office buildings, and their complex.

2. Change Log

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

3. Model Specification

Model & Feature	E18C
Display	7" IPS
Touch Screen	√
Button	X
Housing Material	Plastic
Relay Out	2
Relay In	3
RS485	√
PoE	√
Resolution	1024x600
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	6.0W
POE Full Load Consumption	11W
Power Adapter Standby Power	5.8W
Power Adapter Full Load Consumption	10.35W
Color Option	Black

4. Introduction to Configuration Menu

- **Status:** this sections gives you basic information such as product information, Network Information, and account information etc.
- **Account:** this section concerns SIP account, SIP server, proxy server, transport protocol type, outbound proximity server.
- **Network:** this section mainly deals with DHCP&Static IP setting, and device deployment etc.
- **Intercom:** this section covers Intercom call setting, call log etc.
- **Surveillance:** this section includes audio&video related settings such as Live stream, RTSP, ONVIF, MJPEG.
- **Access Control:** this section includes input type setting, relay setting, door access control in terms private PIN code, Facial recognition, RF card, and BLE setting as well log related configurations such as door log and temperature log.
- **Device:** this section concerns LED light setting, ODSP Setting, screen saver setting, sound&volume setting and third-party integration in terms of integration via Wiegand, RS485.
- **Setting:** this second deals with time &language setting, security notification settings and door prompt text setting.
- **Upgrade:** this section covers Firmware upgrade, device reset&reboot, configuration file auto-provisioning, PCAP.
- **Security:** this section is for Password modification, tamper alarm, and web interface automatic-logout.

- **Mode selection :**

1. **Discovery mode:** It is a plug and play configuration mode. Akuvox devices will configure themselves automatically when users power on the devices and connect them to network. It is super time-saving mode and it will greatly bring users convenience by reducing manual operations. This mode requires no prior configurations previously by the administrator.
2. **SmartPlus mode:** Akuvox SmartPlus is an all-in-one management system. Akuvox SmartPlus is the mobile service that allows audio, video, remote access control between smart phones and Akuvox intercoms. All configurations in the device will be issued automatically from cloud. If users decide to use Akuvox Smartplus please contact Akuvox technical support, and they will help you configure the related settings before using.
3. **SDMC mode:** SDMC (**SIP Device Management Controller**) is a simple and comprehensive software for building management. It provides a topography for a community while offering you a graphical configuration interface for the door access, intercom, monitoring, alarm etc.,. It is a convenient tool for property manager to manage , operate and maintain the community.

- **Tool selection**

Akuvox has many configuration tools for you to set up devices more conveniently. Here we list some common tools, please contact your administrator to get the tool if you need them.

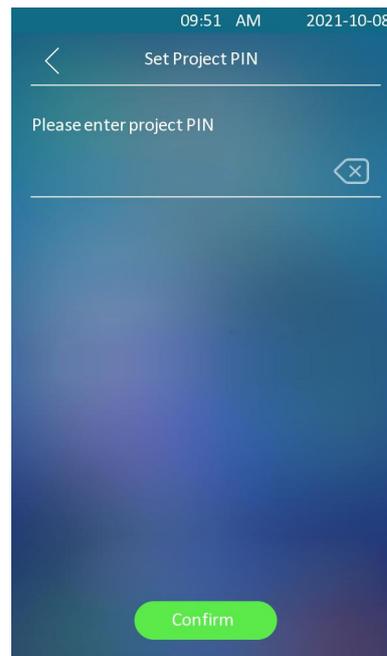
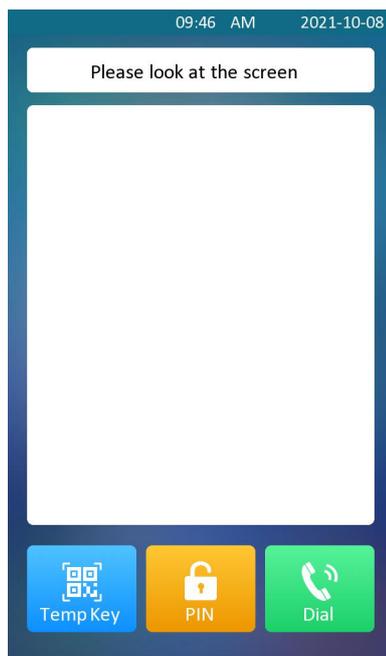
1. **SDMC:** SDMC is suitable for the management of Akuvox devices large communities, including access control, resident information, remote device control etc.,.
2. **Akuvox Upgrade tool:** Upgrade Akuvox devices in batch on a LAN (**Local Area Network**).
3. **Akuvox PC Manager:** Distribute all configuration items in batch on a LAN.
4. **IP scanner:** it is used to search Akuvox device IP addresses on a LAN.
5. **FacePro:** Manage face data in batch for the door phone on a LAN.

5. Access the Device

E18 series door phoneinal system setting can be either accessed on the device directly or on the device web interface.

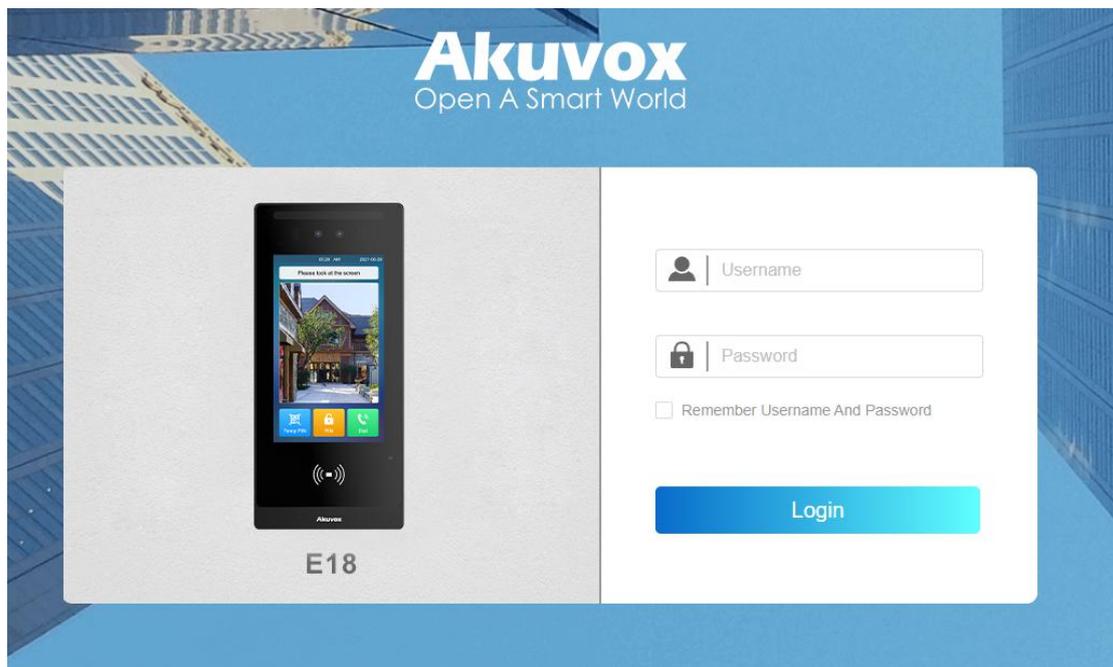
5.1. Access the Device Setting on the device

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



5.2. Access the Device Setting on the Web Interface

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



Tip:

- You can also obtain the device IP address using the Akuvox IP scanner to log in 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?highlight=ip%20scanner>

**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.

6. Time and Language Setting

6.1. Language Setting

When you first set up the device, you might need to set the language to your needs, or you can do it later if needed. And the language can either be set up directly on the device or on the device web interface according to your preference.

6.1.1. Language Setting on the Device

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



6.1.2. Language Setting on the Device Web Interface.

To configure the language on the web interface. Path:**Setting >Time/Lang > LCD Language**.



Parameter Set-up:

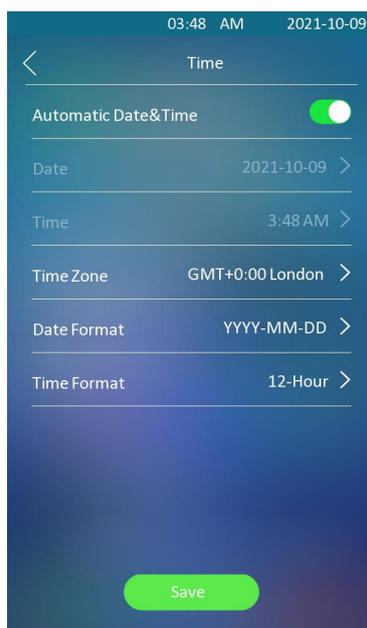
- **Type:** choose a suitable web language. Normally, English is the default web and LCD language.

6.2. Time Setting

Time setting can be set up on the device and on the device web interface in terms of time zone, date and time format etc.

6.2.1. Configure Time Setting on the Device

Time setting on the web interface allows you to set up time and date manually while allowing you to use 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 selected so that the NTP server can synchronize the selected time zone setting to your device. Path:**Display&Sounds > Language**.



Parameter Set-up:

- **Automatic Date&Time:** Automatic Date&Time is toggled on by default, which allows the date& time to be automatically set up and synchronized with the default time zone and the NTP server (**Network Time Protocol**). You can also set it up manually by toggling off the switch first then enter the time and date you want before pressing the **Save** tab for the validation.
- **Date:** click on **Date** to set the date.
- **Time:** click on **Time** to set the time.
- **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 GMT+0.00**.
- **Date Format:** select the date format as you like among three format options: "M-D-Y"; "D-M-Y"; "Y-M-D" and then press the **Confirm** tab for the confirmation.
- **Time Format:** you can either select 12 hour or 24-hour time format as you like, and then press the Confirm tab for the confirmation.

 **Note:**

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

6.2.2. Time Setting on the Device Web Interface

You can configure time setting on the web interface. Path :**Setting > Time/Lang > Time.**

Time

Automatic Date&Time Enabled	<input checked="" type="checkbox"/>
Time Zone	<input type="text" value="GMT+0:00 London"/>
Preferred Server	<input type="text" value="0.pool.ntp.org"/>

Parameter Set-up:

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

Note:

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

6.3. LED Setting

6.3.1. 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 to have the LED light on the card reader area to stay on, you can also set the timing for the exact time span during which the LED light can be disabled in order to reduce the electrical power consumption. Path: **Device > Light > LED of Swiping Card Area**.

Device >> Light

LED Of Swiping Card Area

Enabled

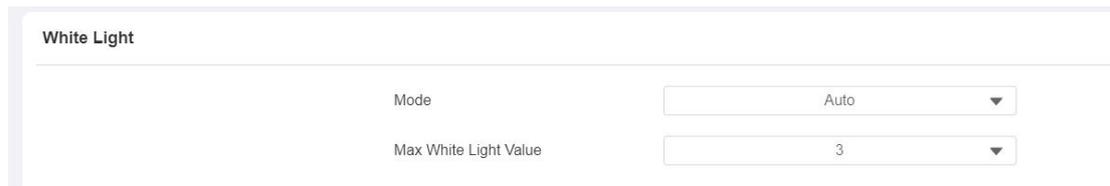
Start Time - End Time(Hour) - (0-23)

Parameter set-up:

- **Enabled:** Tick the check box if 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, e.g. if the time span is from **18-22** it means LED light will stay on during the time span from **6:00 pm to 10:00 pm** during one day (24 hours).

6.3.2. Configure LED White Light Setting

LED White light is used to reinforce the lighting for facial recognition as well as for the QR code access as needed in the dark environment. You can set the white light function properly on the device web interface. Path: **Device > Light > White Light**.



The screenshot shows a configuration panel titled "White Light". It contains two settings:

Parameter	Value
Mode	Auto
Max White Light Value	3

Parameter Set-up:

- **Mode:** select "**Auto**" or "**OFF**". If you select "**Auto**" then the white light will turn on for 5 minutes for facial recognition and QR code scan. And if you select "**Off**" then the white light will be turned off.
- **Max White Light Value:** set the white light value from **1-5**, and the default white light value is "**3**". The greater value it is, the brighter the light will be.

Note:

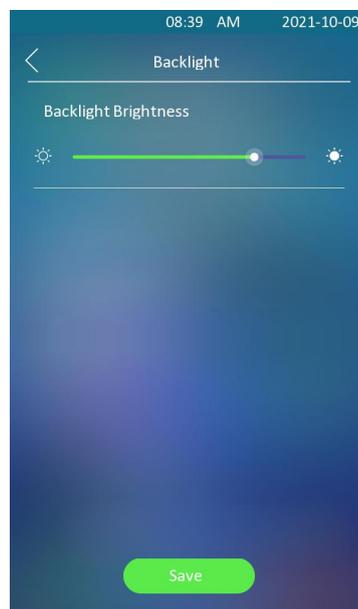
- IR LED light should be triggered first before the white light can be valid in the facial recognition, however IR LED light does not need to be triggered for the white light function in the QR code scan.

6.4. LCD Screen Brightness Setting

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

6.4.1.LCD Screen Brightness Setting on the Device

You can adjust the screen brightness on the device. Path: **Display&Sounds > Backlight**.



6.4.2.LCD Screen Brightness Setting on the Web Interface

You can adjust the screen brightness on the web interface, you can go to **Device > Light > Screen Backlight Brightness**.



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

6.5. Screen Display configuration

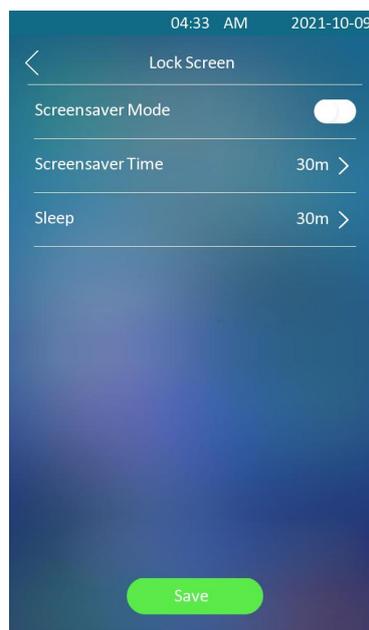
E18C door phones allow you to enjoy a variety of screen displays to enrich your visual and operational experience through the customized setting to your preference.

6.5.1. Configure Screensaver

Screensaver configuration is for the screen protection when the device goes into idle status. You can make the device to go into idle status for a predefined time span when there is no operation on the device or no one is detected approaching. You can configure the screensaver on device and the device web interface.

6.5.2. Configure Screensaver on the Device

You can configure the screensaver on the device directly. Path: **Display&Sounds > Screensaver > Lock Screen.**



Parameter Set-up:

- **Screensaver Mode:** move the toggle switch to the right to enable the screen saver function.
- **Screensaver Time:** set the screensaver duration after the device goes in to sleep mode. The default setting is 30 min.
- **Sleep:** set the screen saver start time range from "10" min. to " 30" min, for example, if you set it as " 10 m" then the device will go into screen saver mode in 10 min. when when there is no operation on the device or no one is detected approaching

6.5.3. Configure Screensaver on the Web Interface

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

Device >> LCD

Standby Interface Display

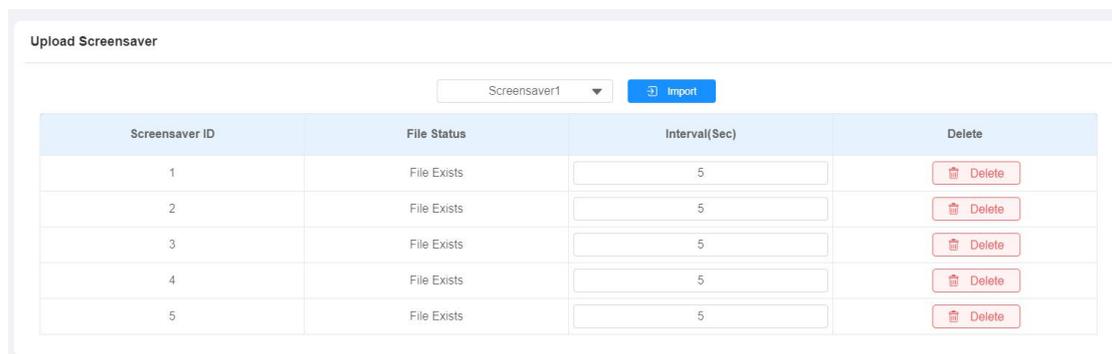
Screensaver Mode	<input checked="" type="checkbox"/>
Screensaver Time	30minutes ▼
Sleep	30minutes ▼

Parameter Set-up:

- **Screensaver Mode:** move the toggle switch to the right to enable the screen saver function.
- **Screensaver Time:** set the screensaver duration after the device goes in to sleep mode. Screensaver duration ranges from 5 seconds to 2 hours on the web interface. While the default setting is 30min.
- **Sleep:** set the screen saver start time range from "10" min. to " 30" min, for example, if you set it as " 10 m" then the device will go into screen saver mode in 10 min. when when there is no operation on the device or no one is detected approaching.

6.5.4. Customize Screensaver on the Web Interface

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



Parameter Setup:

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



Note:

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

6.5.5.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	<input type="text"/>	Speed Dial ▼	<input type="text"/>
2	<input type="text"/>	PIN ▼	<input type="text"/>
3	<input type="text"/>	Call ▼	<input type="text"/>

Parameter Set-up:

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

6.6. Volume & Tone Configuration

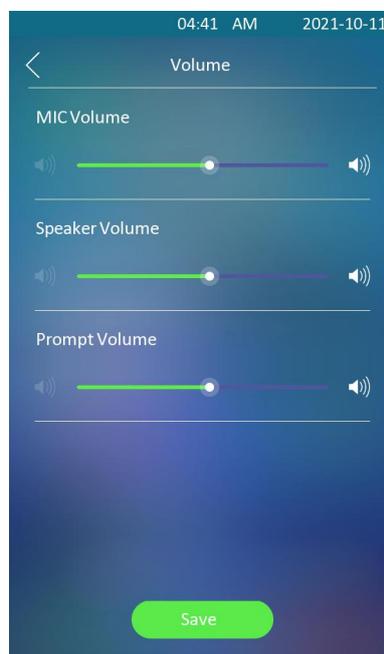
Volume and tone configuration in E18 door phone refers to the Call volume(speaker), Mic volume, prompt volume (eg. open door tone) Moreover, you can upload the tone you like to enrich your personalized user experience.

6.6.1. Volume Configuration

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

6.6.1.1. Configure Volume on the Device

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



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

6.6.1.2. Configure Volume on the Web Interface

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

Volume Control		
Mic Volume	<input type="text" value="8"/>	(1-15)
Speaker Volume	<input type="text" value="8"/>	(1-15)
Tamper Alarm Volume	<input type="text" value="8"/>	(1-15)
Prompt Volume	<input type="text" value="8"/>	(0-15)

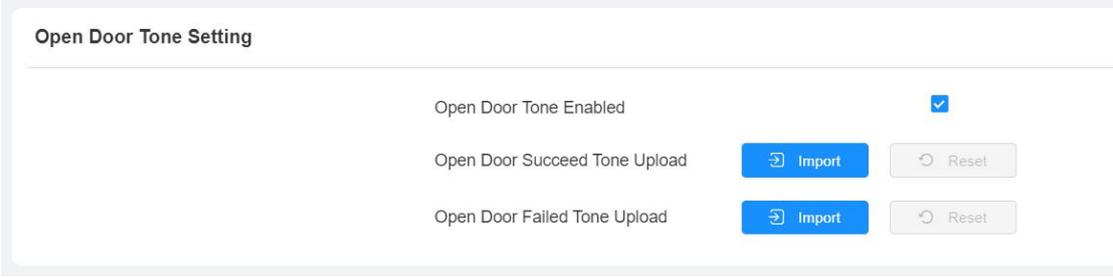
Parameter Setup:

- **Mic Volume:** set the mic volume from 0-15 according to your need. The default Mic volume is "8".
- **Speaker Volume:** set the speaker volume from 0-15 according to your need. The default speaker volume is "8"..
- **Tamper Alarm Volume:** set the tamper alarm volume from 0-15 according to your need. The default volume is "8".
- **Prompt Volume:** adjust the prompt volume, which includes various types of prompt sound for door open success and failure, ringback, and temperature measurement sound etc.
- **Tamper Alarm Volume:** set the tamper alarm volume from 0-15 according

to your need. The default volume is "8".

6.6.2. Upload Open Door Tone

You can upload the **Open Door Tone** on the device web interface. Path: **Device > Audio > Open Door Tone Setting**.

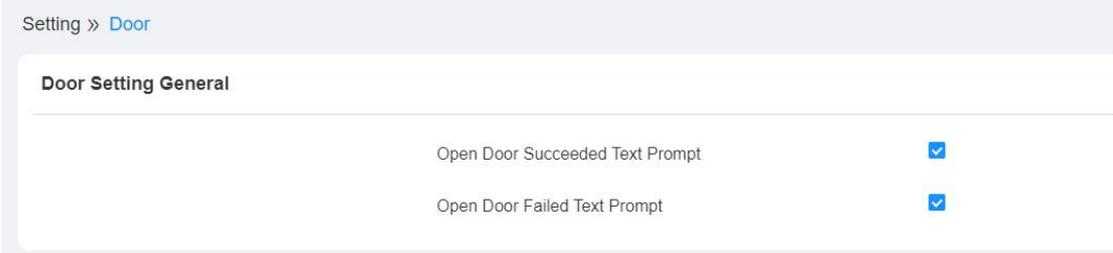


The screenshot shows the 'Open Door Tone Setting' page. It features three rows of settings:

Setting	Control
Open Door Tone Enabled	<input checked="" type="checkbox"/>
Open Door Succeed Tone Upload	<input type="button" value="Import"/> <input type="button" value="Reset"/>
Open Door Failed Tone Upload	<input type="button" value="Import"/> <input type="button" value="Reset"/>

6.6.3. Configure Door Open Prompt Text

You can enable or disable the door open prompt to be shown on the device's screen for door open failure and success. Path: **Setting > Door > Door Setting General**.



The screenshot shows the 'Door Setting General' page. It features two rows of settings:

Setting	Control
Open Door Succeeded Text Prompt	<input checked="" type="checkbox"/>
Open Door Failed Text Prompt	<input checked="" type="checkbox"/>

Parameter Setup:

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

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

6.6.4. Configure Hang-up Tone

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

Hang Up Tone Setting

Hang Up Tone Enabled

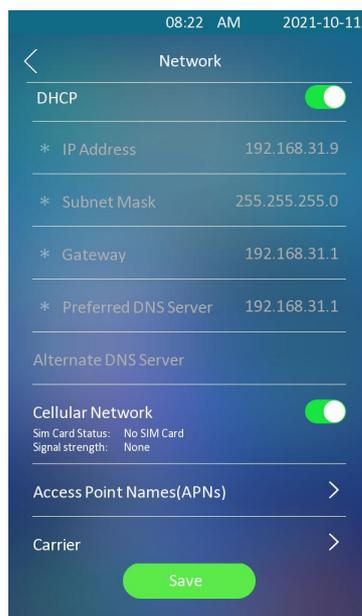
Hang Up Tone Upload

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

7. Network Setting

7.1. Device Network Connection Setting

You can configure the default DHCP mode (**Dynamic Host Configuration Protocol**) and static IP connection. More over, you can set up IP address, Subnet Mask, Default Gateway, and DNS servers.



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 servers address have to be manually configured according to your actual network environment.
- **IP Address:** set up the IP Address if the static IP mode is selected.
- **Subnet Mask:** set up the subnet Mask according to your actual network

environment.

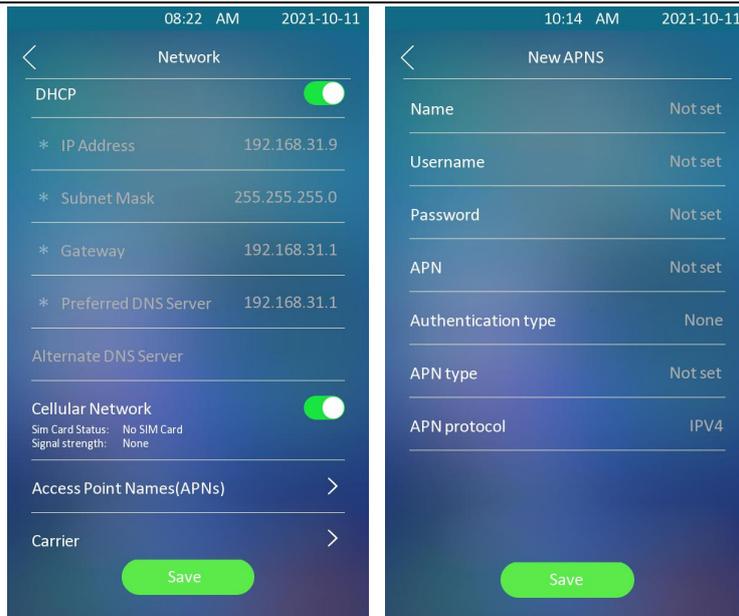
- **Default Gateway:** set up the correct gateway default gateway according to the IP address of the default gateway.
- **Preferred&Alternate DNS Server:** set up preferred or alternate DNS Server (**Domain Name Server**) according to your actual network environment. Preferred DNS server is the primary 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.

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

The screenshot shows the 'LAN Port' configuration page. At the top, there is a breadcrumb trail: 'Network >> Basic'. Below this, the title 'LAN Port' is displayed. The main configuration area includes a 'Type' section with two radio buttons: 'DHCP' (unselected) and 'Static IP' (selected). Below the radio buttons are six input fields for the following parameters: 'IP Address', 'Subnet Mask', 'Default Gateway', 'Preferred DNS Server', and 'Alternate DNS Server'. Each field is currently empty.

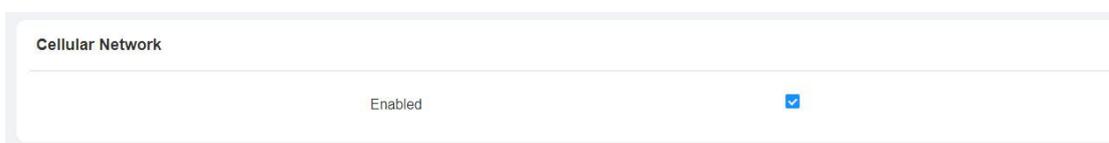
7.2. LTE Wireless Connection Setting

In addition to Ethernet network connection, the device is installed with a LTE module which allows both users and installers to conduct a convenient, quick, 4G wireless connection in the installation environment with no access to wired network such as old building etc. Path: **Network > Cellular Network**.



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

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



7.3. Device Local RTP configuration

For the device network data transmission purpose, device needs to be set up with a range of RTP port (**Real-time Transport Protocol**) for establishing an

exclusive range of data transmission in the network. Path:**Network > Advanced > Local RTP** interface.

Local RTP

Starting RTP Port	<input type="text" value="11800"/>	(1024-65535)
Max RTP Port	<input type="text" value="12000"/>	(1024-65535)

Parameter set-up:

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

7.4. Device Deployment in Network

E18 should be deployed before they can be properly configured in the network environment in terms of their location, operation mode, address and extension numbers for the device control and the convenience of the management. Path:**Network > Advanced > Connect Setting**.

Connect Setting

Server Mode	SDMC	
Discovery Mode	<input checked="" type="checkbox"/>	
Device Node	<input type="text" value="1"/>	
Device Extension	<input type="text" value="1"/>	
Location	<input type="text" value="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** or **Cloud** and **None**. **None** is the default factory setting indicating the device is not in any server type, therefore you are allowed to choose Cloud, SMDC in discovery mode.
- **Discovery Mode:** click "**Enabled**" to turn on the discovery mode of the device so that it can be discovered by other devices in the network, and click "**Disabled**" if you want to conceal the device so as not to be discovered by other devices.
- **Device Node:** specify the device address by entering device location information from the left to the right :**Community, Unit, Stair, Floor, Room** in sequence.
- **Device extension:** enter the device extension number for the device you installed
- **Location:** enter the location in which the device is installed and used.

7.5. NAT Setting

NAT (**Network Address Translation**) allows hosts in an organization's private intranet to transparently connect to hosts in the public domain. There is no need for internal hosts to have registered Internet addresses. It is a way to translate the internal private network IP address into a legal network IP address technology. The NAT in the device web is limited to maintaining a connection with the remote SIP server. The principle is to send a heartbeat message to the remote SIP server at a set interval after the function is turned on. Otherwise, the server may judge that the device is offline and allocate the SIP assigned to other devices, resulting in failure to connect to it in the future. Path: **Account > Advanced > NAT**.

The screenshot shows the NAT configuration page. It has a title 'NAT' at the top left. Below the title, there are three settings:

- UDP Keep Alive Messages:
- UDP Alive Messages Interval: (5-60Sec)
- RPort Enabled:

Parameter Set-up:

- **UDP Keep Alive Messages:** If enabled, the device will send out the message to the SIP sever so that SIP sever will recognize that the device is in on-line 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 Area Network**).

8. Intercom Call Configuration

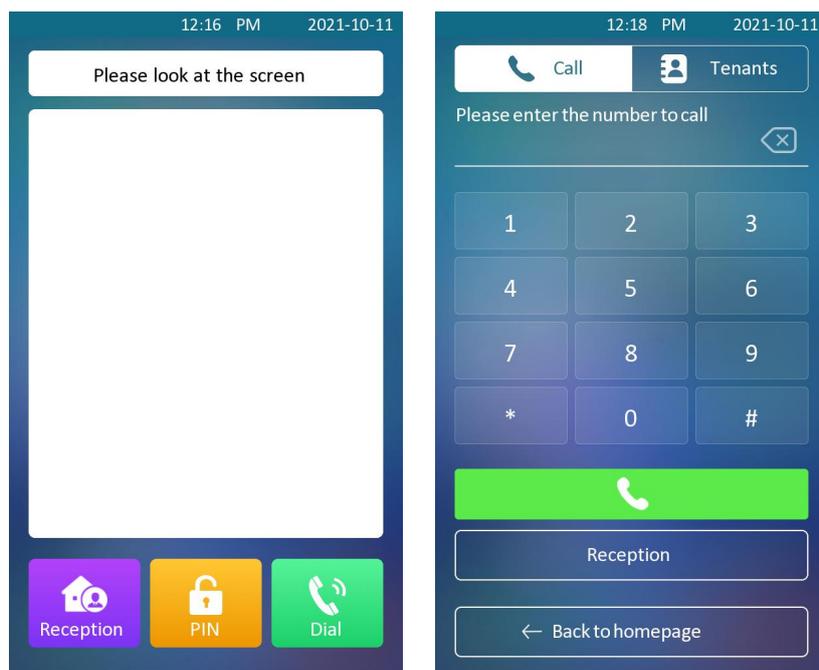
Intercom call in the device can be configured to allow you to perform a variety of customized intercom calls such as IP call and SIP call for different application scenarios.

8.1. IP call & IP Call Configuration

IP call 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.

8.1.1. Make IP/SIP calls

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



8.1.2. IP Call Configuration

You are required to set up a specific port for the data transmission for the IP calls. Path: **Intercom > Basic > Direct IP**.

Intercom >> Basic

Direct IP

Enabled

Port (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 call 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**. And you enter any values within the range other than the 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.

8.2. SIP Call & SIP Call Configuration

SIP calls (**Session Initiation Protocol**) are established and supported by SIP servers. If the two intercom devices want to initiate SIP calls with each other, then they should be registered in the same SIP server. And SIP call parameters related to its account, server, and transport type need to be configured first before you can make calls on the device.

You can make 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.



Note:

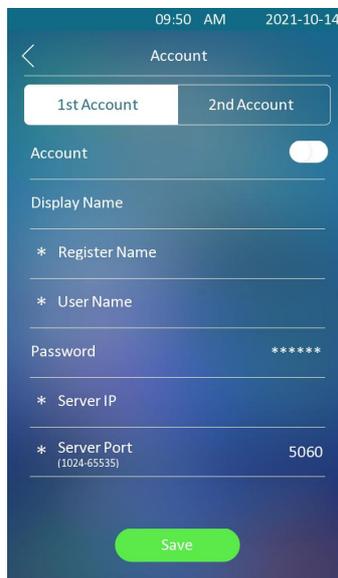
- Akuvox currently has its own PBX called My PBX server, and it has also achieved compatibility with third-party PBX, you can refer to the URL <https://www.akuvox.com/PartnersTechnology.aspx?ptype=16> below:

8.2.1.SIP Account Registration

E18 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.

8.2.1.1. Configure SIP Account on the Device

To configure SIP account on the device. Path: **Account**.



Parameter Set-up:

- **Display Name:** configure the name, for example the device's name to be shown on the device being called to.
- **Register Name:** enter the SIP account register Name obtained from the SIP account administrator.

- **User Name:** enter the user name obtained from SIP account administrator.
- **Password:** enter the password obtained from the SIP account administrator.
- **Server IP:** enter the SIP server address for the SIP account selected.
- **Server port:** enter the SIP server port for communication. The SIP port is "5060" by default.

8.2.1.2. Configure SIP Account on the Web Interface

To configure the configuration on the web interface, you go to **Account > Basic > SIP Account** interface.

The screenshot shows the 'SIP Account' configuration page. It contains the following fields and controls:

Status	Disabled
Account	Account1
Account Enabled	<input type="checkbox"/>
Display Label	<input type="text"/>
Display Name	<input type="text"/>
Register Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>

Parameter Set-up:

- **Status:** check to see if the SIP account is registered or not.
- **Account:** select the exact account (Account 1&2) to be configured .

- **Account Enabled:** tick the checkbox to enable or disable registered SIP account.
- **Display Name:** configure the name, for example the device's name to be shown on the device being called to. You can fill in 63 bytes of characters in length maximum
- **Display Label:** configure the device label to be shown on the device screen. You can fill in 63 bytes of characters in length maximum
- **Register Name:** enter the SIP account register Name obtained from the SIP account administrator. You can fill in 63 bytes of characters in length maximum.
- **User Name:** enter the user name obtained from SIP account administrator. You can fill in 63 bytes of characters in length maximum
- **Password:** enter the password obtained from the SIP account administrator. You can fill in 63 bytes of characters in length maximum.

8.2.2. SIP Server Configuration

You are required to enter the SIP port for the device's SIP account registration and for SIP calls. Path: **Account > Basic > Preferred SIP Server**

Preferred SIP Server

Server Address	<input type="text"/>	
Sip Server Port	<input type="text" value="5060"/>	(1024-65535)
Registration Period	<input type="text" value="1800"/>	(30-65535 Sec)

Alternate SIP Server

Server Address	<input type="text"/>	
Sip Server Port	<input type="text" value="5060"/>	(1024-65535)
Registration Period	<input type="text" value="1800"/>	(30-65535 Sec)

Parameter Set-up:

- **Server Address** (preferred SIP server) : enter the primary server IP address number or its URL.
- **Server Address** (alternate SIP server): enter the backup SIP server IP address or its URL.
- **SIP Server Port:** set up 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.

8.2.3. Configure SIP Ports for SIP Calls

You are required to set up a SIP port range for making SIP calls.

Call	
Max Local SIP Port	<input type="text" value="5062"/> (1024-65535)
Min Local SIP Port	<input type="text" value="5062"/> (1024-65535)

Parameter Setup:

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

8.2.4. 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 call session

via port-based data transmission. Path: **Account > Basic > Outbound Proxy Server**.

Outbound Proxy Server

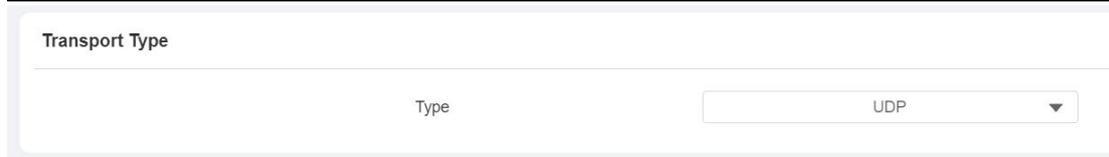
Outbound Enabled	<input type="checkbox"/>
Preferred Server IP	<input type="text"/>
Port	<input type="text" value="5060"/> (1024-65535)
Alternate Server IP	<input type="text"/>
Port	<input type="text" value="5060"/> (1024-65535)

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 establish call session via the outbound proxy server
- **Alternate Server IP**: set up Backup Server IP for the back up outbound proxy server.
- **Port**: enter the Port number for establish call session via the backup outbound proxy server.

8.2.5. Configure Data Transmission Type

SIP message 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 from. Path: **Account > Basic > Transport Type**.



Transport Type

Type

Parameter Set-up:

- **UDP:** select “UDP” for unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
- **TCP:** select “TCP” for Reliable but less-efficient transport layer protocol.
- **TLS:** select “TLS” for Secured and Reliable transport layer protocol.
- **DNS-SRV:** select “DNS-SRV” to obtain DNS record for specifying the location of services. And **SRV** not only records the server address but also the server port. Moreover, SRV can also be used to configure the priority and the weight of the server address.

8.3. Dial Options Configuration

E18 offers a variety of Dial options that allows you to have fast dial experience while relieving you off memory burden due to long and complex dial numbers.

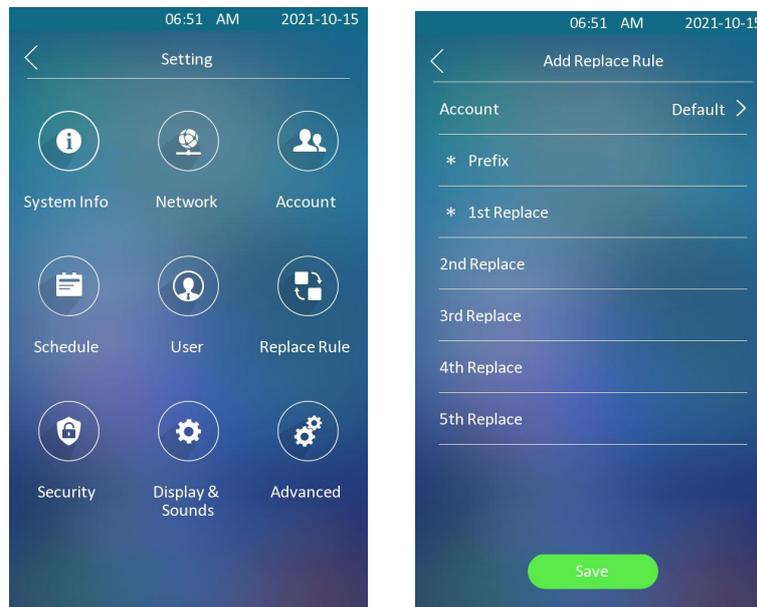
8.3.1. Quick Dial by Number Replacement

If you want to replace the long and complex dial number with a shorter number that can be memorized at greater ease and convenience for making calls, you can configure the dial number replacement on the device and on the device web interface. You can replace a multiple device dial numbers such as IP address or SIP numbers with only one short number.

8.3.2. Quick Dial By Number Replacement on the Device

You can replace the long SIP/IP number with the short number on the device.

Path: **Replace Rule > Add Replace Rule.**

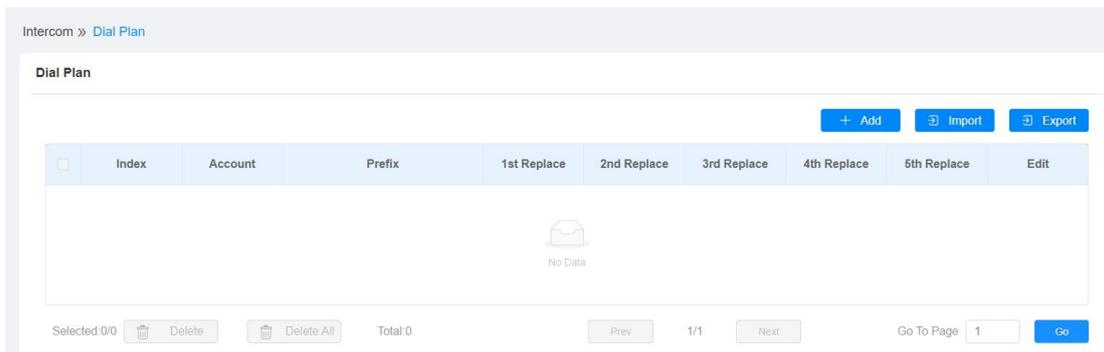


Parameter Set-up:

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

8.3.2.1. Quick Dial by Number Replacement on the Device

You can replace the long SIP/IP number with the short number on the web interface. Path: **Intercom > Dial Plan.**

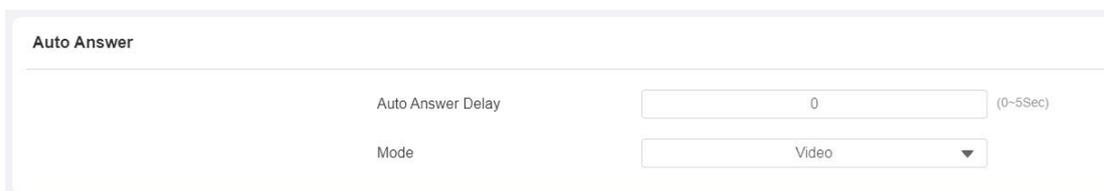


8.4. Call Auto-answer Configuration

Auto-answer is a function that allows you to answer the incoming call without picking up the phone. When auto-answer is enabled, the incoming call will be answered automatically based on the answering timing you defined.

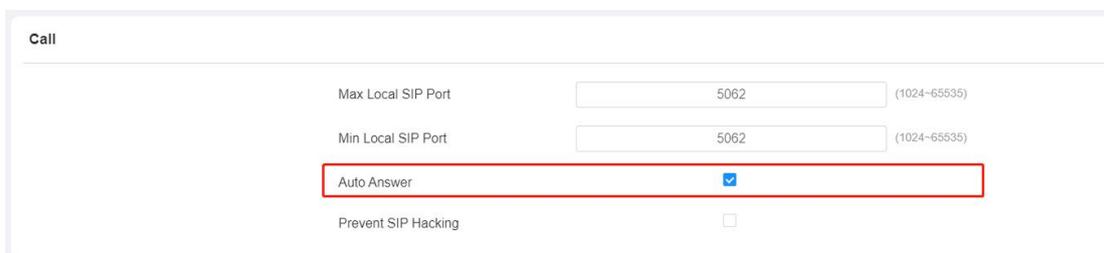
➤ Configure auto-answer function

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



➤ Enable Auto-answer mode

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



Parameter Set-up:

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

8.5. Call Settings

8.5.1. Maximum Call Duration Setting

E18C door phone allows you to set up the call time duration in receiving the call from the calling device as the caller side might forget to hang up the phone. When the call time duration is reached, the door phone will terminate the call automatically. Path: **Intercom > Call Feature > Max Call Time**

Intercom >> Call Feature

Max Call Time

Max Call Time (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:

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

8.5.2. Maximum Dial Duration Setting

Maximum Dial duration is consisted of 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 hang up the call if the call is not answered by the door phone. In contrary, Maximum dial-out time refers to the maximum time duration before the door phone hang up itself automatically when the call from the door phone is not answered by the intercom device being called to. Path: **Intercom > Call Feature> Max Dial Time.**

Max Dial Time		
Dial In Time	<input type="text" value="60"/>	(30~120Sec)
Dial Out Time	<input type="text" value="60"/>	(30~120Sec)

Parameter set-up:

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

in 60 seconds. 60 seconds is the dial in time duration by default.

- **Dial Out Time:** enter the dial in time duration for your door phone (**ranging from 5-120 sec.**) for example, if you set the dial out time duration is 60 seconds in your door phone, then the door phone will hang out the call it dialed out automatically if the call is not answered by the device being called to.

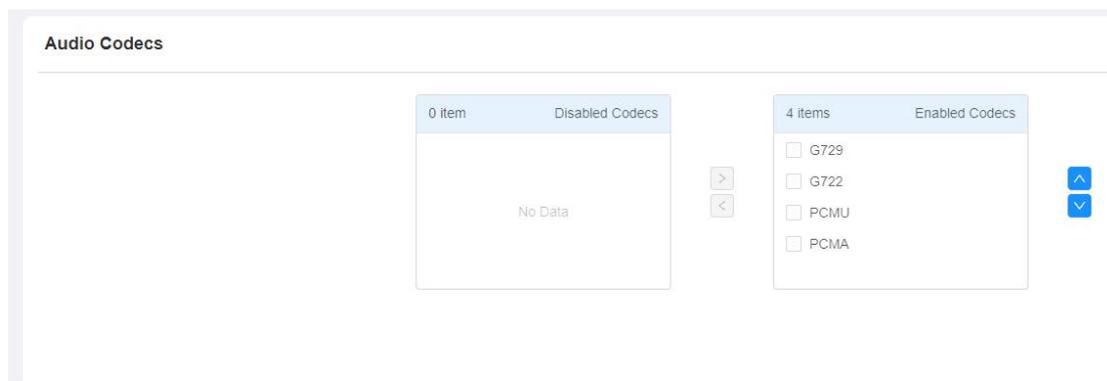
**Note:**

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

8.5.3. Audio & Video Codec Configuration for SIP Calls

8.5.3.1. Configure Audio Codec

E18C door phone support four types of Codec (PCMU, PCMA, G729, G722) for encoding and decoding the the audio data during the call session. Each type of Codec vary in terms of the sound quality. You can select the specific codec with different bandwidth and sample rate flexibly according to the actual network environment. Path: **Account > Advanced > Audio Codecs**.

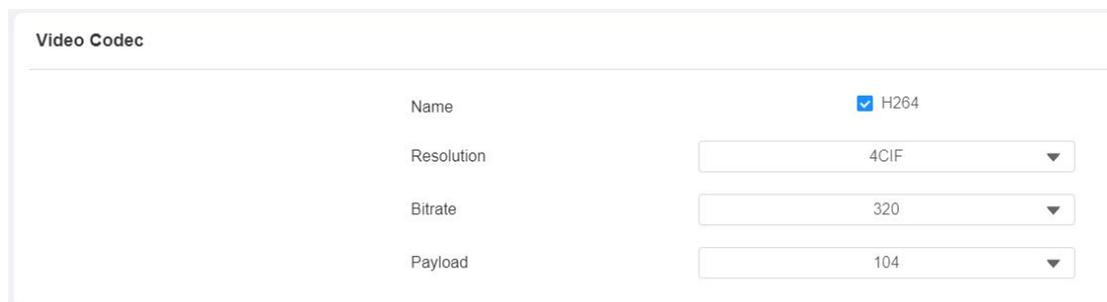


Please refer to the bandwidth consumption and sample rate for the four types of codecs below:

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

8.5.3.2. Configure Video Codec

This series supports H.264 codec that provides a better video quality at much lower bit rate with different video quality and payload. Path : **Account > Advanced > Video Codecs**.



Parameter set-up:

- **Name:** Check to select the H264 video codec format for the door phone video stream. H264 is the video codec by default.
- **Resolution:** select the code resolution for the video quality among 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 in 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 pay load between the door phone and the corresponding intercom device should be identical. The default payload is 104.

8.6. Configure DTMF Data Transmission

In order to achieve the 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 device for the third party integration. Path: **Account > Advanced > DTMF**

The screenshot shows a configuration panel titled "DTMF". It contains three settings:

- Mode:** A dropdown menu currently showing "RFC2833".
- DTMF Code Transport format:** A dropdown menu currently showing "Disabled".
- Payload:** A text input field containing "101", with a range "(96-127)" indicated to its right.

Parameter set-up:

- **Mode:** select DTMF mode among five options: "Inband", "RFC2833", "Info+Inband" and "Info+RFC2833" based on the specific DTMF

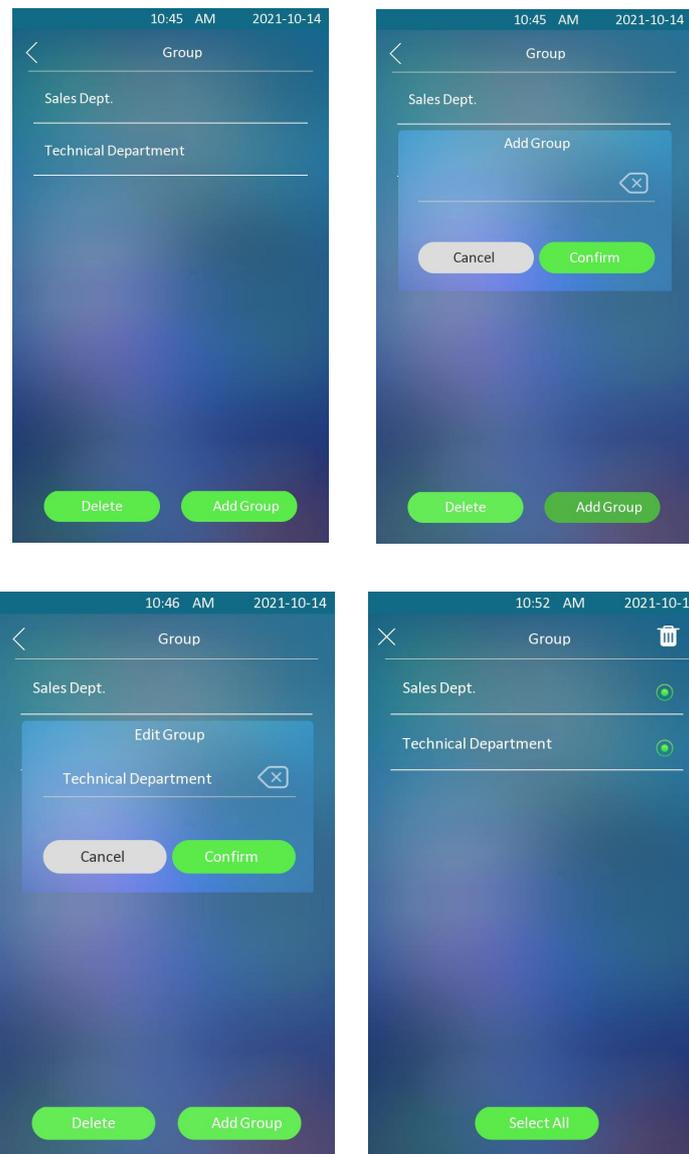
transmission type of the third party device to be matched with as the party for receiving signal data.

- **How to Notify DTMF:** select among four types: "**Disable**" "**DTMF**" "**DTMF-Relay**" "**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 the the specific data transmission payload agreed on between the sender and receiver during the data transmission.

9. Phone Book Configuration

9.1. Phone Book Configuration on the Device

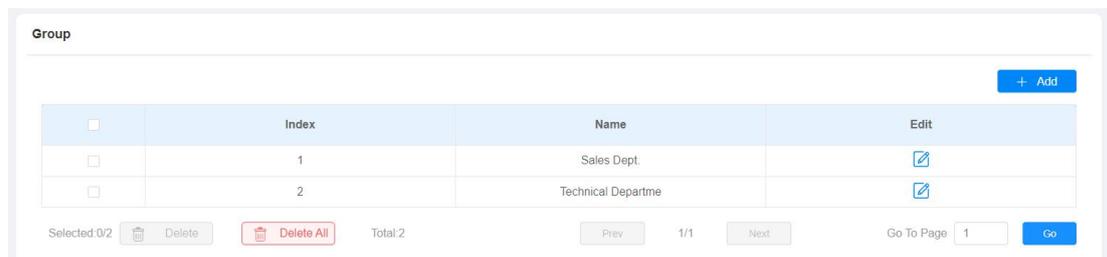
You can configure the contacts list in terms of adding and modifying contact groups or contacts on the device directly. To configure the phone book on the device **User > Group**



9.2. Phone Book Configuration on the Web Interface

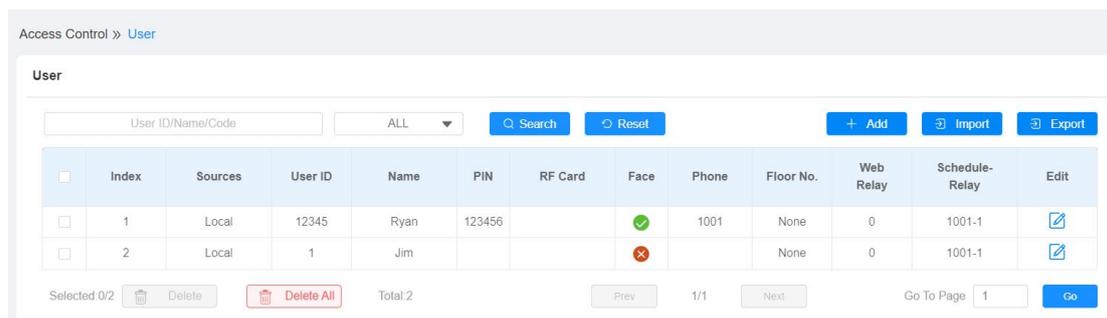
9.2.1. Manage Contact Groups on the Web Interface

You can configure contact and contact groups by adding and editing them on the web interface Path: **Access Control > User> Group** .



9.2.2. Contact List Configuration on the Web Interface

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



9.2.2.1. Contact List Display Setting

If you want to customize your contact list display to your desired visual preference. You can go to the web interface to do the configuration. To configure the configuration on the web interface. Path: Intercom > **Basic >**

Tenants List > Tenants List Setting.

Tenants List Setting

Show Tenants Of Local Group Enabled	<input checked="" type="checkbox"/>
Show Cloud Tenants Enabled	<input checked="" type="checkbox"/>
Tenants Sort By	ASCII Code
Click Tenants To Dial Out	<input checked="" type="checkbox"/>
Hide Group Label For Local Tenants List	<input type="checkbox"/>

Parameter Set-up:

- **Show Tenants of Local Group Enabled:** tick or untick the check box to control the display the of the group label. If you untick the check box, then only the group tab will be displayed while the contact tab will be concealed and vice versa.
- **Show Cloud Tenants Enabled:** tick the check box to show the cloud tenants in the tenants list. And when you untick the check box, the cloud tenants will be concealed.
- **Tenants Sort By:** select ASCII Code 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 sort according to their room numbers.
- **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 the 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 vise versa.

10. Relay Switch Setting

10.1. Relay Switch Setting

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

Access Control » Relay

RelayA

Trigger Delay(Sec)	<input type="text" value="0"/>
Hold Delay(Sec)	<input type="text" value="5"/>
DTMF Mode	<input type="text" value="1 Digit DTMF"/>
1 Digit DTMF	<input type="text" value="0"/>
2~4 Digits DTMF	<input type="text" value=""/>
Relay Status	Low
Relay Name	<input type="text" value="RelayA"/>

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 triggered until 5 seconds after you press "unlock " tab.
- **Hold Delay (Sec):** set the relay hold delay timing (Ranging from 1-10 Sec.) For example, if you set the hold delay time as " 5" Sec. then the relay will be delayed for 5 after the door is unlocked.
- **DTMF Mode:** select the number of DTMF digit for the door access control (Ranging from 1-4 digits) For example, you can select 1 digit DTMF code or 2-digit DTMF code etc., according to your need.
- **1-digit DTMF :** set the 1-digit DTMF code within range from (0-9 and *,#).
- **2~4 Digits DTMF:** set the DTMF code according to the **DMTP Option** setting. For example, you are required to set the 3-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 the convenience.

 **Note:**

- Only the external devices connected to the relay switch needs to be powered by powered adapters as 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** field. And if you set DTMF mode from 2-4 in **2~4 Digits DTMF**" field, you can not edit DTMF code in **1 Digit DTMF** field.

10.2.DTMF Code Configuration

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

Parameter Set-up:

DTMF

Mode	<input type="text" value="RFC2833"/>
DTMF Code Transport format	<input type="text" value="Disabled"/>
Payload	<input type="text" value="101"/> (96-127)

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



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.

10.3.Web Relay Setting

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

10.3.1. 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, password. And you can fill in a maximum of 50 web relay action commands for different web relay actions, which can later selected on the device screen for the specific relay action for

the door access control. Path: **Access Control > Web Relay**

Access Control » Web Relay

Web Relay

Type:

IP Address:

Username:

Password:

Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>

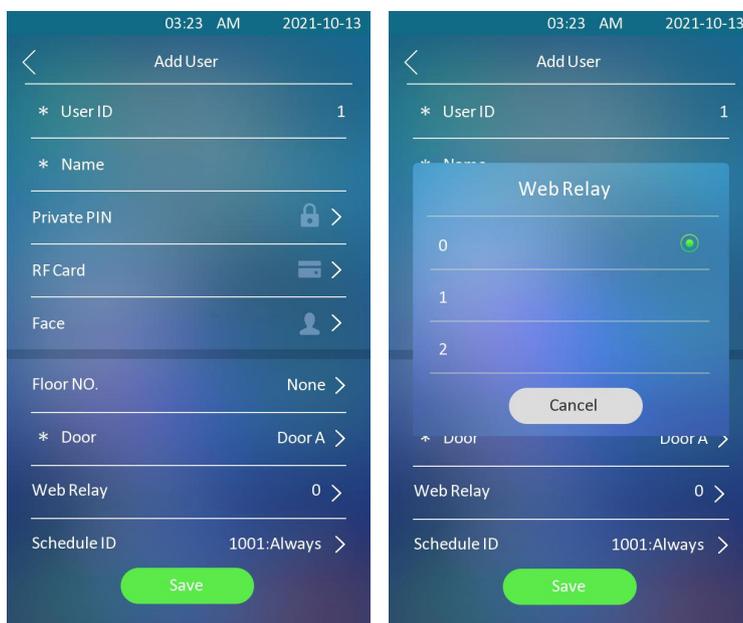
Parameter Set-up:

- **Type:** select 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.
- **IP Address:** enter the we 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 is authenticated via HTTP and you can define the passwords using **“http get”** in Action.
- **Web Relay Action:** enter the specific web relay action command provided by the web manufacturer for different actions by the web relay.
- **Web Relay Key:** enter the configured DTMF code, when the door is unlock via DTMF code, the action command will be sent to the web relay automatically.
- **Web Relay Extension:** enter the relay extension information, which can be a SIP Account user name of an intercom device such as an indoor monitor, so that the specific action command will be sent when unlock is performed on the intercom device, while this setting is optional. And please refer to the example below:

[http://admin:admin@192.168.1.2/state.xml?relayState=2.](http://admin:admin@192.168.1.2/state.xml?relayState=2)

10.3.2. Configure Web Relay on the Device

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



10.4. Relay Schedule

You can set the specific relay to be always opened in specific time range during which time the door will stay open, allowing residents to gain door entry without applying any types of door access credentials to unlock the door. This feature is designed for some specific scenarios such as the time after school, or for morning work time.

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

Directory » Schedule

Schedule

ALL + Add Import Export

<input type="checkbox"/>	Index	Schedule ID	Sources	Mode	Name	Date	Day Of Week	Time	Edit
<input type="checkbox"/>	1	1001	Local	Daily	Always			00:00-23:59	
<input type="checkbox"/>	2	1002	Local	Daily	Never			00:00-00:00	
<input type="checkbox"/>	3	1	Local	Normal	Ryan	20211013-20211014	Sunday,Monday,Tuesday,Wednesday,Thursday,Friday,Saturday	00:00-23:59	
<input type="checkbox"/>	4	2	Local	Normal	Relay Schedule 1	20211013-20211014	Sunday,Monday,Tuesday,Wednesday,Thursday,Friday,Saturday	00:00-23:59	

Add Schedule X

Name

Mode

Date Range -

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

Date Time -

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

Relay Schedule

Relay ID

Schedule Enabled

1/13 items Unselected

- 1001:Always
- 1002:Never
- 1:Ryan
- 2:Relay Schedule 1
- 3:Dayshift

0 item Selected

No Data

Note:

You can refer to the chapter 11.1 **Create Door Access Schedule** for the relay schedule setting as the configuration of relay schedule is identical to the

11. Door Access Schedule Management

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

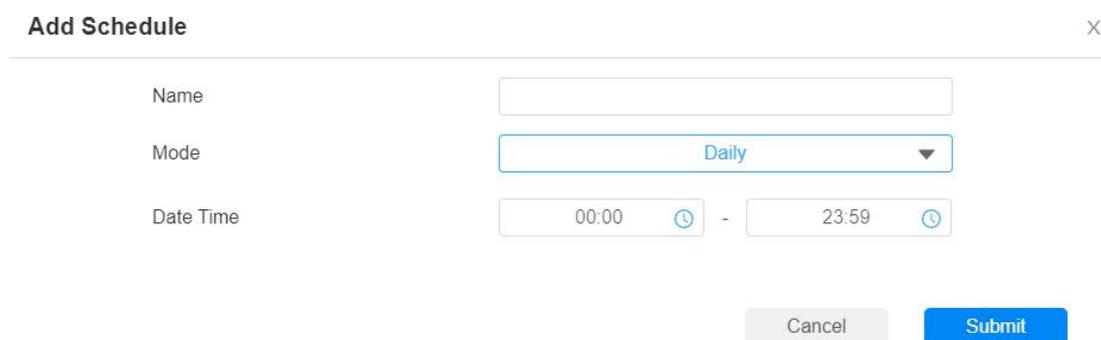
11.1. Configure Door Access Schedule

You can create door access schedules so that they can be later conveniently applied to the door access control intended for individual user or a group of users created. More over, you can edit your door access schedule if needed. You can manage the door access schedule on the device and the device's web interface.

11.1.1. Create Door Access Schedule on the Web Interface

You can create the door access schedule on the daily or monthly basis and you can also create schedule that allows you to plan for a longer period of time in addition to running the door access schedule on the daily or monthly basis. Path: **Access Control > Schedule**.

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



The screenshot shows a web form titled "Add Schedule" with a close button (X) in the top right corner. The form contains three main input fields:

- Name:** A text input field.
- Mode:** A dropdown menu currently set to "Daily".
- Date Time:** Two time selection fields. The first is set to "00:00" and the second is set to "23:59", with a minus sign between them.

At the bottom right of the form, there are two buttons: a grey "Cancel" button and a blue "Submit" button.

Parameter Setup:

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

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

Add Schedule X

Name	<input style="width: 80%;" type="text"/>
Mode	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block; background-color: #f0f0f0;">Weekly ▼</div>
Day Of Week	<input checked="" type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input checked="" type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input checked="" type="checkbox"/> Saturday <input checked="" type="checkbox"/> Sunday <input type="checkbox"/> Check All
Date Time	<div style="display: flex; align-items: center; gap: 10px;"> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">00:00 🕒</div> - <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">23:59 🕒</div> </div>

Cancel
Submit

Parameter Setup:

- **Name:** enter the schedule name.
- **Mode:** select daily schedule.
- **Day of Week:** Select the day (s) on which door access can be valid on a weekly basis.
- **Date Time:**Set up the time schedule for the validity of the door access during a day.

To create a longer period schedule, you can do as follows:

Add Schedule
✕

Name

Mode Normal ▼

Date Range 2021-10-13 - 2021-10-14

Day Of Week

<input checked="" type="checkbox"/> Monday	<input checked="" type="checkbox"/> Tuesday	<input checked="" type="checkbox"/> Wednesday
<input checked="" type="checkbox"/> Thursday	<input checked="" type="checkbox"/> Friday	<input checked="" type="checkbox"/> Saturday
<input checked="" type="checkbox"/> Sunday	<input type="checkbox"/> Check All	

Date Time 00:00 - 23:59

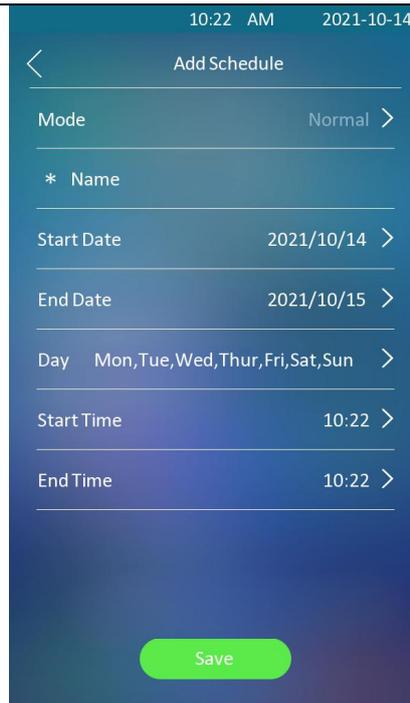
Cancel
Submit

Parameter Setup:

- **Name:** enter the schedule name.
- **Mode:** select Normal schedule.
- **Date Range:** Set the data range of the validity of the door access.
- **Day of Week:** Select the day (s) on which door access can be valid on a weekly basis.
- **Date Time:**Set up the time schedule for the validity of the door access during a day.

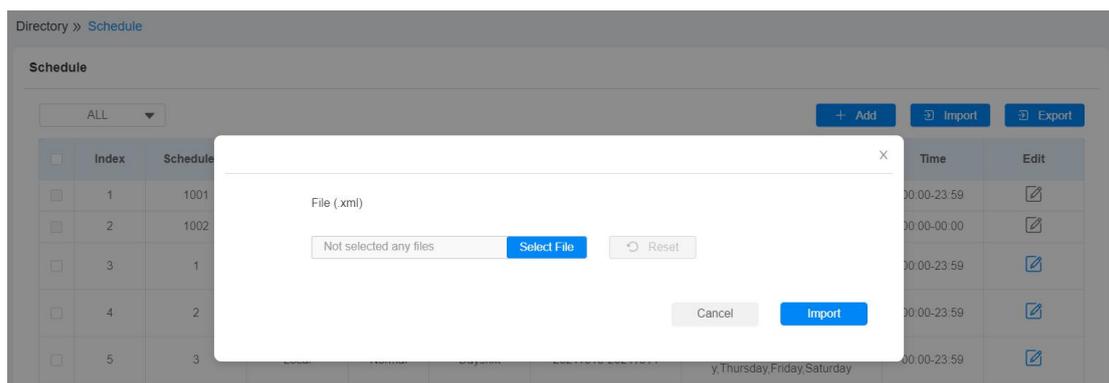
11.1.2. Create Door Access Schedule on the Device.

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



11.1.3. Import and Export Door Access Schedule

In addition to creating door access schedule separately, you can also conveniently import or export the schedules in order to maximize your door access schedule management efficiency. Path: **Access Control > Schedule**.



Note:

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

11.1.4. Edit the Door Access Schedule

11.1.4.1. Edit the Door Access Schedule on the Web Interface

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

Directory » Schedule

Schedule

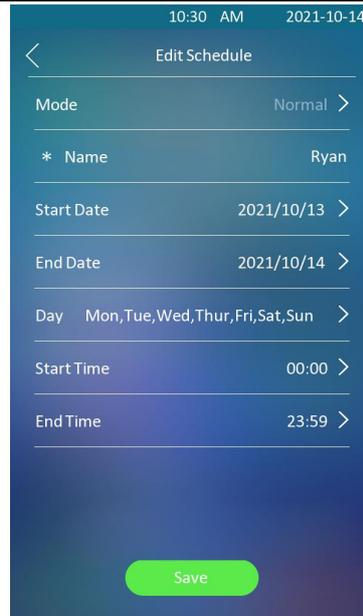
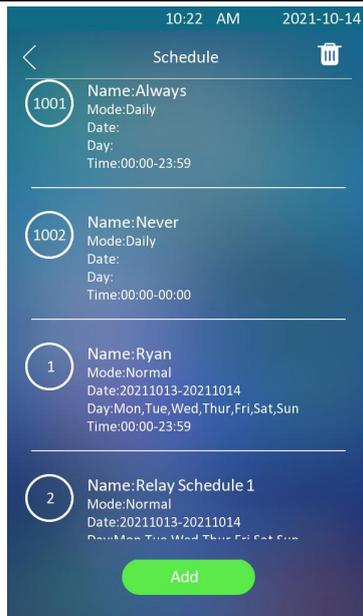
ALL + Add Import Export

<input type="checkbox"/>	Index	Schedule ID	Sources	Mode	Name	Date	Day Of Week	Time	Edit
<input type="checkbox"/>	1	1001	Local	Daily	Always			00:00-23:59	
<input type="checkbox"/>	2	1002	Local	Daily	Never			00:00-00:00	
<input type="checkbox"/>	3	1	Local	Normal	Dayshift	20211013-20211014	Sunday,Monday,Tuesday,Wednesday,Thursday,Friday,Saturday	00:00-23:59	
<input checked="" type="checkbox"/>	4	2	Local	Normal	Dayshift	20211013-20211014	Sunday,Monday,Tuesday,Wednesday,Thursday,Friday,Saturday	00:00-23:59	
<input type="checkbox"/>	5	3	Local	Normal	Dayshift	20211013-20211014	Sunday,Monday,Tuesday,Wednesday,Thursday,Friday,Saturday	00:00-23:59	
<input type="checkbox"/>	6	4	Local	Normal	Dayshift	20211013-20211014	Sunday,Monday,Tuesday,Wednesday,Thursday,Friday,Saturday	00:00-23:59	
<input type="checkbox"/>	7	5	Local	Normal	Dayshift	20211013-20211014	Sunday,Monday,Tuesday,Wednesday,Thursday,Friday,Saturday	00:00-23:59	

Selected: 1/7 Delete Delete All Total: 7 Prev 1/1 Next Go To Page 1 Go

11.1.4.2. Edit the Door Access Schedule on the Device

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



12. Door Unlock Configuration

E18 offers you three types of door access via PIN code, NFC, RF card and Facial recognition. You can configure them on the device and web interface. More over, you can import or exporting the configured files to maximize your RF card configuration efficiency.

12.1. Configure PIN Code for Door Unlock

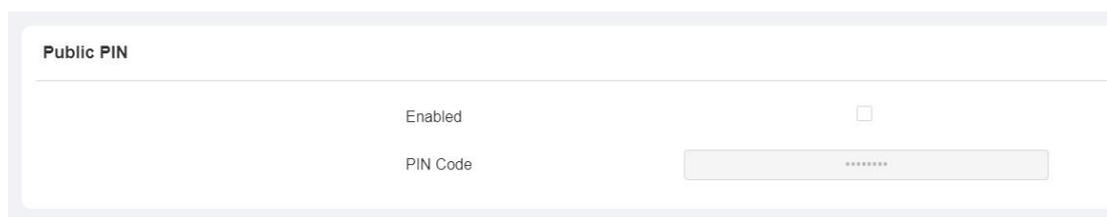
You can create and modify both public PIN code and private PIN code for the door access on E18 door phone.

12.1.1. Configure Public PIN code

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

- Configure public PIN code on the web interface

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



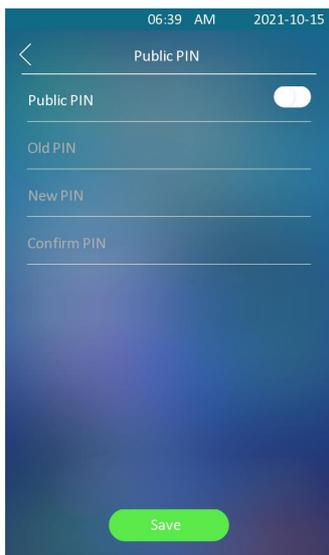
The screenshot shows a web interface for configuring the Public PIN. It features a title 'Public PIN' at the top left. Below the title, there are two rows of configuration options. The first row is labeled 'Enabled' and has a checkbox that is currently unchecked. The second row is labeled 'PIN Code' and has a text input field containing seven asterisks (*****).

Parameter Setup:

- Enabled: Tick the checkbox to enable the Public PIN code application.
- PIN Code: set the PIN code with digit limit ranging from "4-8".

- Configure public PIN code on the device

Path: **Security > Public PIN.**



 **Note:**

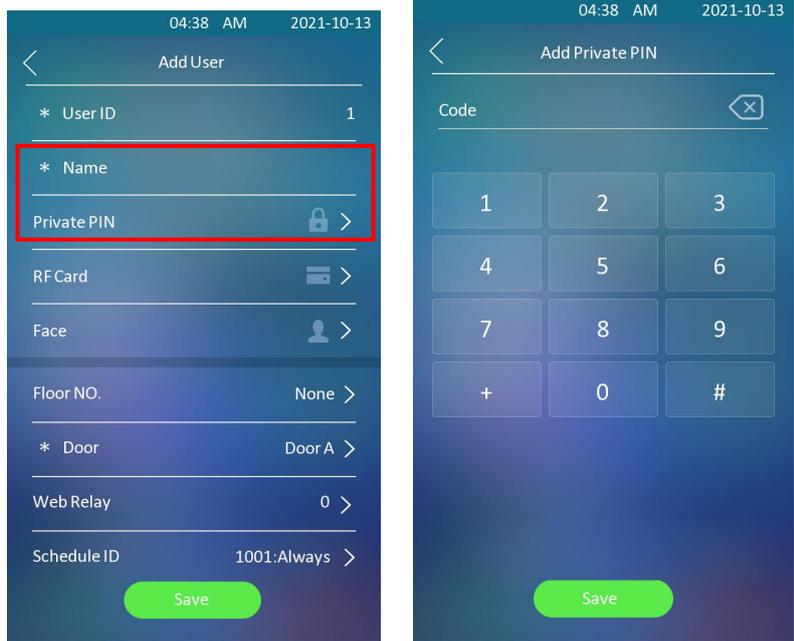
- Public PIN code will not valid until the function is turned on.

 **Note:**

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

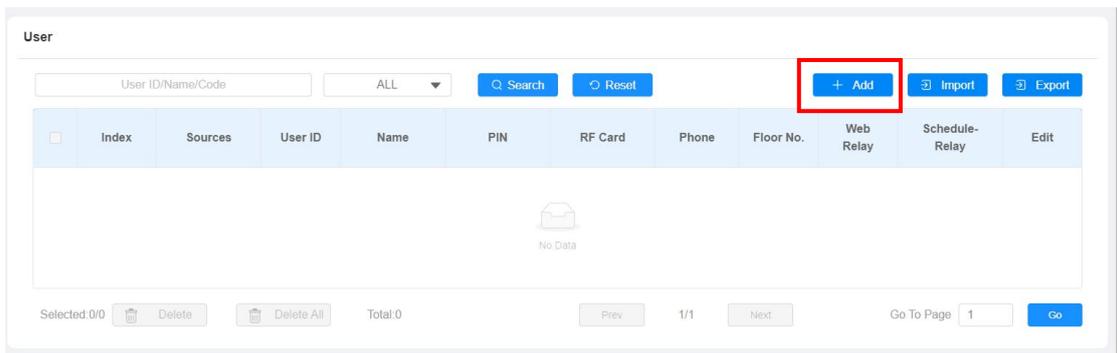
12.1.2. Configure Private PIN Code on the Device

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**



12.1.3. Configure Private PIN Code on the Web Interface

On the web interface, you can not only set up 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. Path: **Access Control > User**.



User » Add User

User Info

User ID

Name

PIN

Code

Parameter Set-up:

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

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

Access Setting

Relay RelayA RelayB

Floor No.

Web Relay

Schedule

1/12 Items	Unselected	1 Item	Selected
<input type="checkbox"/> 1001:Always		<input type="checkbox"/> 3.Dayshift	
<input type="checkbox"/> 1002:Never			
<input type="checkbox"/> 1:Ryan			
<input type="checkbox"/> 2:Relay Schedule 1			
<input checked="" type="checkbox"/> 4:Dayshift			

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 credentials as they are identical in configuration.

12.1.4. Configure Private PIN Access Mode

E18 offers you two types of access modes for private PIN code access, namely "PIN" and "APT#+PIN". Path: **Access Control > PIN Setting > Private PIN**

Parameter Set-up:

- **Authorization Mode:** select access mode between "PIN" and "APT#+PIN". if you select "PIN" then you are only required to enter 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.

12.2. Configure RF Card for Door Unlock

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

12.2.1. Configure RF Card on the Web Interface

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

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 the door access.

12.2.1.1. 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 with that applied in the third party system. **Path: Access Control > Card setting >RFID.**

Access Control » [Card Setting](#)

RFID

IC Card Display Mode

ID Card Display Mode

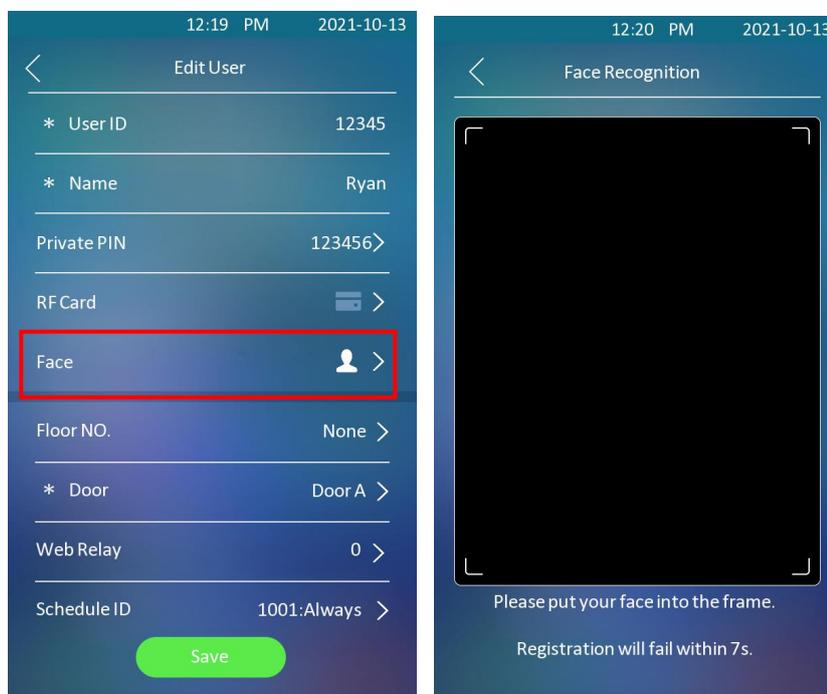
Parameter Set-up:

IC/ID 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.

12.2.2. Configure Facial Recognition for Door Unlock

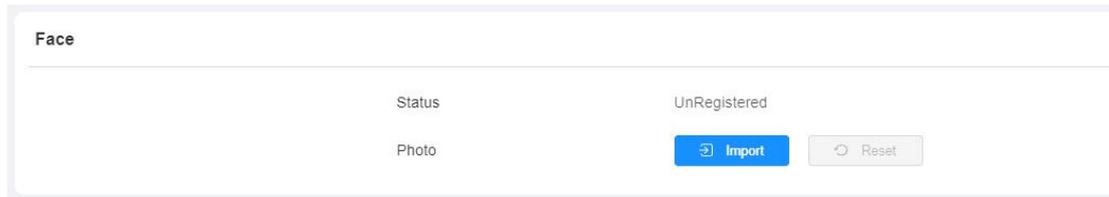
12.2.2.1. Configure Facial Recognition on the Device

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



12.2.2.2. Configure Facial Recognition on Web Interface

You can import the face data to the device on the web interface. Path: **Access Control > User > Face**.



Face

Status	UnRegistered
Photo	<input type="button" value="Import"/> <input type="button" value="Reset"/>

Parameter Set-up:

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



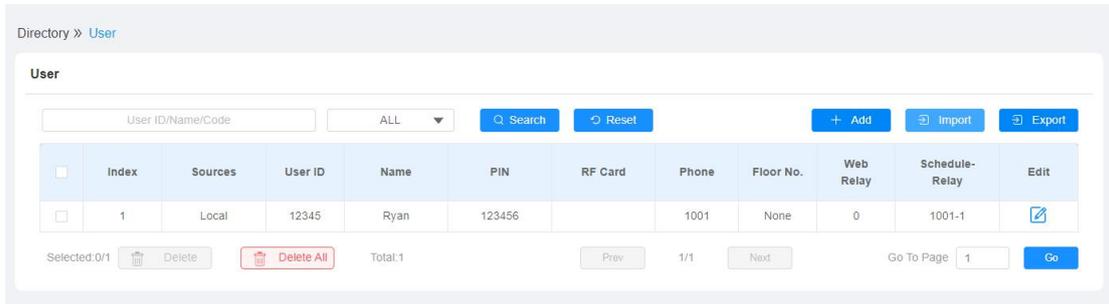
Note:

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

12.3. Configure Door Access Using Configured Files.

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

in number. Path: **Access Control > User > User.**

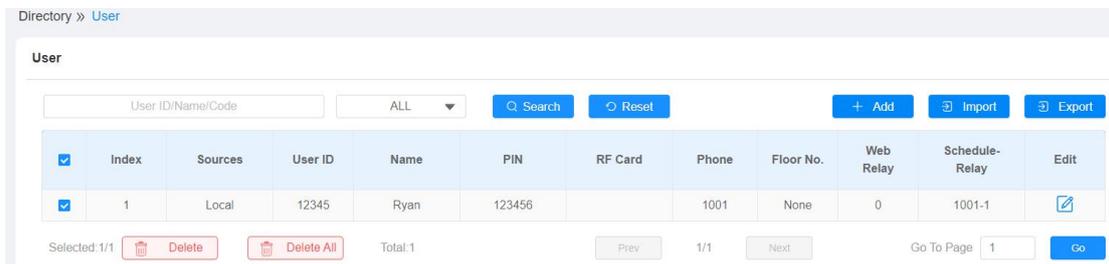


Note:

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

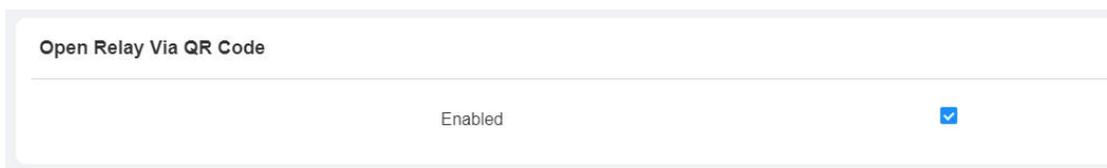
12.4. Edit the User(s)-specific door access data

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



12.4.1. Unlock by QR Code

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



Open Relay Via QR Code

Enabled

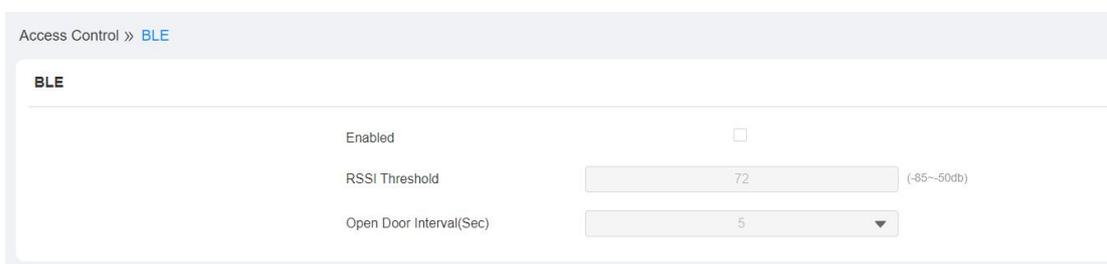


Note:

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

12.4.2. 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 door phone for the door access. Path: **Access Control > BLE > BLE**.



Access Control >> BLE

BLE

Enabled

RSSI Threshold (-85~-50db)

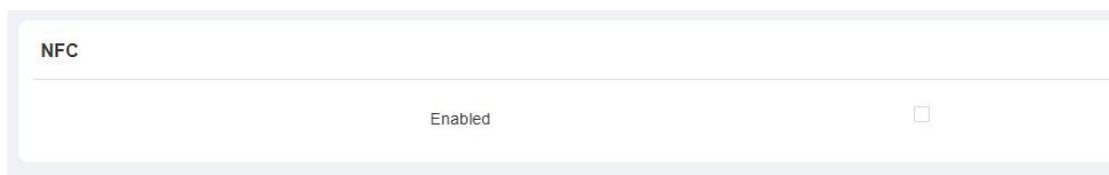
Open Door Interval(Sec)

Parameter Set-up:

- **Enabled:** enable or disable the Bluetooth function. Bluetooth is turned off by default.
- **Rssi Threshold:** select the signal receiving strength from -85~-50db in absolute terms. The higher value it is, the greater strength it has. The default value is 72db in absolute terms.
- **Open Door Interval:** select the time interval between the every two Bluetooth door accesses.

12.4.3. Unlock by NFC

You can also gain the 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 the door access. Path: **Access Control > Card Setting> NFC**



Parameter Set-up:

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

12.4.4. 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 the HTTP command (URL) on the web browser to trigger the relay when you are not available by the door for the door access. Path: **Access Control > Relay > Open Relay via HTTP**.

Open Relay Via HTTP

Enabled	<input checked="" type="checkbox"/>
Username	<input type="text"/>
Password	<input type="password"/>

Parameter Set-up:

- **Enable:** enable the HTTP command unlock function by clicking on **Enable** field.
- **User Name:** enter the user name of the device web interface, for example "Admin".
- **Password:** enter the password for the HTTP command. For example : "12345".

Please refer to the following example:

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



Note:

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

12.4.5. 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 device's Input to trigger the relay for the door access. Path: **Access Control > Input > Input**.

Input A

Enabled	<input checked="" type="checkbox"/>
Trigger Electrical Level	Low ▼
Action To Execute	<input type="checkbox"/> FTP <input type="checkbox"/> TFTP <input type="checkbox"/> Email <input type="checkbox"/> HTTP <input type="checkbox"/> SIP Call
HTTP URL	<input style="background-color: #eee;" type="text"/>
Action Delay	0 (0-300Sec)
Execute Relay	None ▼
Door Status	Low

Parameter Set-up:

- **Trigger Electrical Level:** select the trigger electrical level options between "High" and "Low" according to the actual operation on the exit button.
- **Action to Execute:** select the method to carry out the action among four options: FTP, Email, HTTP, 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 your press the button.
- **Execute Relay:** set up relays to be triggered by the input.
- **Door Status:** display the status of input signal.

12.4.6. Unlock by Reception Tab

In the device home screen, E18 provide residents and visitors a quick door unlock by pressing the **Reception** tab on the bottom of the home screen.

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

Key Setting

Reception Enabled	<input checked="" type="checkbox"/>
Name	<input type="text" value="Reception"/>
Number	<input type="text"/>

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 to after pressing the Reception icon for the door access.

12.4.7. Body Temperature Measurement for Door Access

E18 provide 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 measurement along with optional mask detection check before they are allowed for the door access.

12.4.7.1. Body Temperature Measurement Configuration

You can configure the body temperature measurement function in terms of defining the normal temperature as well as making schedule for the validity

of the function etc. Path: **Access Control > Body Temperature > Measuring Body Temperature.**

Access Control > [Body Temperature](#)

Measuring Body Temperature

Mode	<input type="text" value="Disabled"/>	
Mask Detection	<input type="text" value="Disabled"/>	
Temperature Unit	<input type="text" value="Fahrenheit"/>	
Normal Body Temperature	<input type="text" value="99.14"/>	(Below 99.14°F)
Low Temperature	<input type="text" value="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	<input type="text" value="Access Denied"/>	
Action For Low Body Temperature	<input type="text" value="Try Again Later"/>	
Action To Execute	<input type="checkbox"/> SIP/ IP Call	

Parameter set-up:

- **Mode:** select either **"Disabled"** Mode **"Wrist"** or **"Forehead"** Mode for temperature measurement according to your need. The device can be installed with digital forehead and wrist temperature detector therefore you 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 mask-wearing prompt only without making the the mask-wearing mandatory. 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 37.3 degree Celsius as the normal

temperature, then any body temperature measured higher than 37.3 degree Celsius will be deemed as abnormal temperature, while the temperature lower than 34 degree Celsius will be deemed as low body temperature.

- Low Temperature: set the low temperature.
- Action For Abnormal Body Temperature:
- Action For Low Body Temperature:
- **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 is 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** field.

13. Security

13.1. Tamper Alarm Setting

Tamper alarm function serves as a protection against any unauthorized removal of the devices by triggering off the temper alarm on the device. Path: **Security > Basic > Temper Alarm.**

The screenshot shows the 'Tamper Alarm' configuration page. It features a table with two rows. The first row has 'Enabled' on the left, a checked checkbox in the middle, and a 'Disarm' button on the right. The second row has 'Key Status' on the left and 'High' in the middle.

Tamper Alarm		
Enabled	<input checked="" type="checkbox"/>	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:** temper alarm will not be triggered unless the key status is shifted from "**Low**" to "**High**" status.



Note:

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

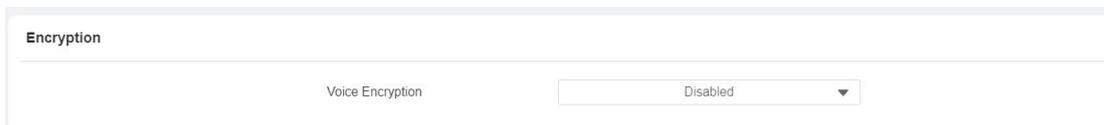


Note:

- The round rubber button at the back of the device must be in press-down status otherwise the alarm will not be fired.

13.2. Voice Encryption

SRTP(Secure Real-time Transport Protocol) is a protocol defined on the basis of Real-time Transport Protocol. The data of the transmission protocol provides encryption, message authentication, integrity assurance and replay protection. Path: **Account > Advanced > Encryption** interface



The screenshot shows a web interface titled "Encryption". Below the title, there is a label "Voice Encryption" followed by a dropdown menu. The dropdown menu is currently set to "Disabled".

Parameter Set-up:

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

13.3. Motion Detection

Motion Detection is often used for unattended surveillance video and automatic alarm. The images collected by the camera at different frame rates will be calculated and compared by the CPU according to a certain algorithm. You can turn enable motion detection and configure the time interval, and configure the motion detection sensitivity and notification type when the motion detection action is triggered.

13.3.1. Configure Motion Detection on the Web Interface

On the device web interface, you can not only configure the time interval but also the motion detection sensitivity and notification type when the motion detection action is triggered. Path: **Surveillance > Motion > Motion Detection Options** interface

Surveillance » Motion

Motion Detection Options

Motion Detection Options

Action To Execute FTP TFTP Email
 HTTP SIP Call

HTTP URL

Timing Interval (1-120Sec)

Detection Accuracy (1-6)

Execute Relay RelayA RelayB

Parameter Set-up:

- **Motion Detection Options:** tick the check box to enable the motion detection function.
- **Action to Execute:** select the action to be executed (FTP、TFTP 、Email 、HTTP、 SIP Call) after motion detection is triggered.
- **HTTP URL:** enter the HTTP URL command which will be sent to the designated server for certain action.
- **Time Interval:** set the time interval in the same away as you do on the device.
- **Detection Accuracy:** set the detection accuracy for the detection sensitivity. The small value it is, the greater sensitivity. the default detection accuracy value is "20".
- **Execute Relay :** select the relay A or relay B to be triggered when then motion detection is triggered.

You can also set the motion detection time schedule.

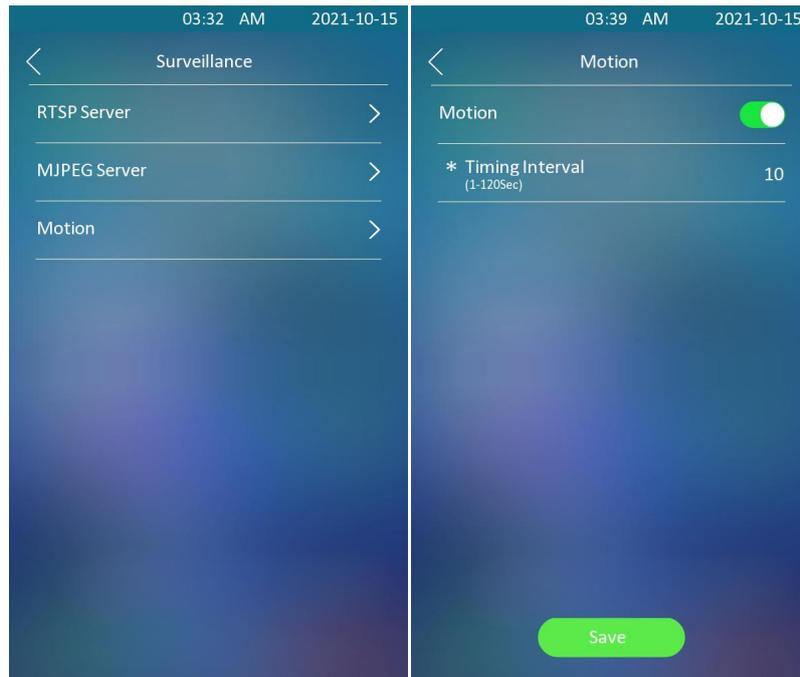
Motion Detect Time Setting

Day Monday Tuesday Wednesday
 Thursday Friday Saturday
 Sunday Check All

Start Time - End Time -

13.3.2. Configure Motion Detection on the Device

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



13.4. Security Notification Setting

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

13.4.1. Email Notification Setting

If you want to receive the security notification via email, you can configure the Email notification on the web interface properly. Path: Setting > Action

Setting » [Action](#)

Email Notification

Senders Email Address	<input type="text"/>
Senders Email Name	<input type="text"/>
Receivers Email Address	<input type="text"/>
Receivers Email Name	<input type="text"/>
SMTP Server Address	<input type="text"/>
Port	<input type="text"/>
SMTP User Name	<input type="text"/>
SMTP Password	<input type="password" value="....."/>
Email Subject	<input type="text"/>
Email Content	<input type="text"/>
Email Test	<input type="button" value="Test Email"/>

Parameter set-up:

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

- **Email content:** compile the emails contents according to your need.
- **Email Test:** click to test if the email can be sent and received.

13.4.2. FTP Notification setting

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

The screenshot shows a web form titled "FTP Notification". It contains four input fields arranged vertically:

- FTP Server: A text input field.
- FTP User Name: A text input field.
- FTP Password: A password input field with a masked password of six asterisks (*****).
- FTP Path: A text input field.

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 FTP server.

13.4.3. TFTP Notification Setting

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



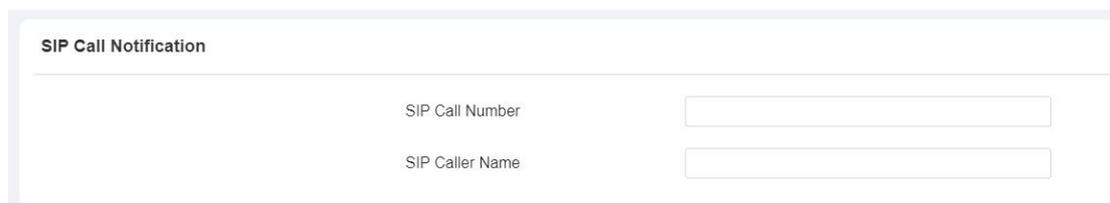
The screenshot shows a web interface titled "TFTP Notification". Below the title is a horizontal line. Underneath, there is a label "TFTP Server" followed by a text input field.

Parameter set-up:

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

13.4.4. 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 > TFTP Notification**.



The screenshot shows a web interface titled "SIP Call Notification". Below the title is a horizontal line. Underneath, there are two labels: "SIP Call Number" and "SIP Caller Name", each followed by a text input field.

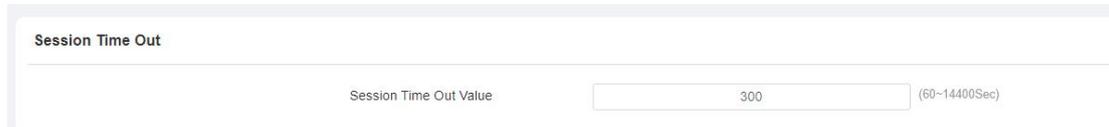
Parameter Set-up:

- **SIP Call Number:** enter the SIP call number.
- **SIP Caller Name:** enter the SIP caller Name.

13.5. 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 the security purpose or for the convenience of operation. Path:**Security > Basic > Session Time Out**.

To configure the web interface time-out, you can do as follows:



The screenshot shows a configuration page titled "Session Time Out". It features a single input field labeled "Session Time Out Value" with the number "300" entered. To the right of the input field, the range "(60~14400Sec)" is displayed. The page has a light gray header and a white body.

Parameter Setup:

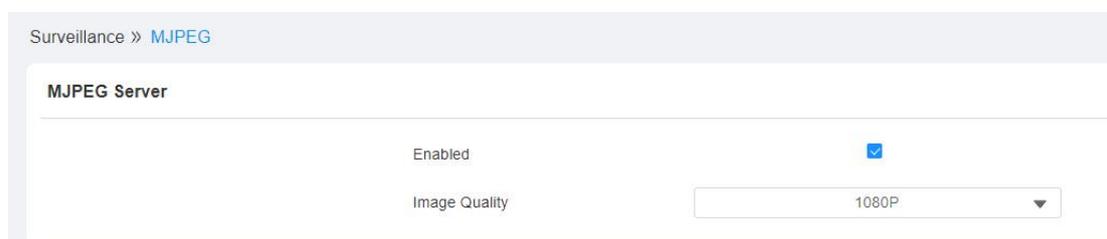
- **Session Time Out Value:** set the automatic web interface logout timing ranging from 60 seconds to 14400 seconds. The default value is 300.

14. Monitor and Image

14.1. Mjpeg Image Capturing

E18C allow 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.

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



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**

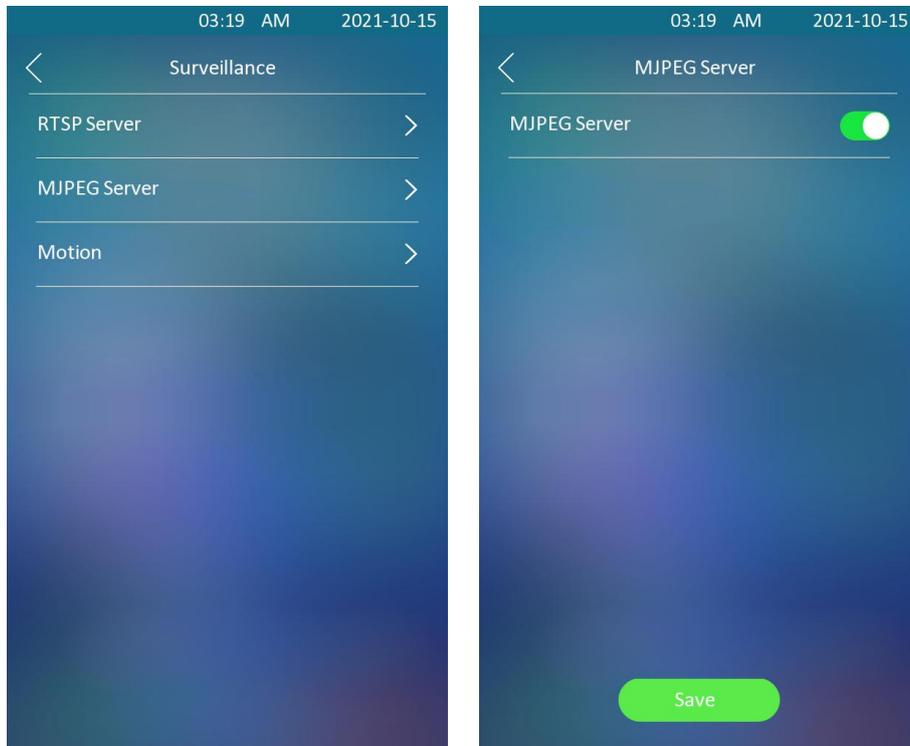
After the Mjpeg service is enabled, you can capture the image from the door phone using following three types of URL format:

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

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

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

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

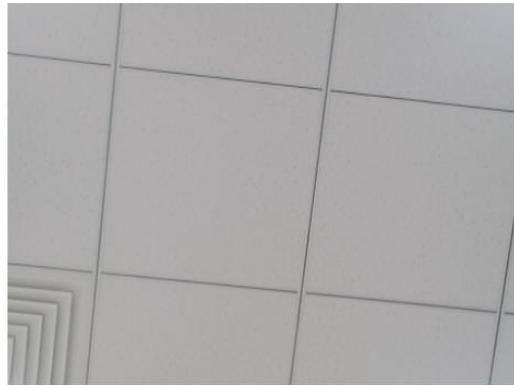


14.2.Live Stream

If you want to check the real-time video from the E18, you can go to the the device web interface to obtain the real-time video or you can also enter the correct URL on the we browser to obtain it directly. Path:**Surveillance > Live Stream.**

Surveillance » [Live Stream](#)

Live Stream

**Note:**

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

14.3. RTSP Stream Monitoring

E18 supports RTSP stream that allows intercom devices such as indoor monitor or the monitoring unit from the third party to monitor or obtain the the real time audio/ video (RTSP stream) from the door phone using the correct URL.

14.3.1. RTSP Basic Setting

You are required to set up RTSP function in terms of RTSP Authorization, authentication and password etc., before you are able to use the function.

Path: **Surveillance > RTSP > RTSP Basic**

Surveillance » RTSP

RTSP Basic

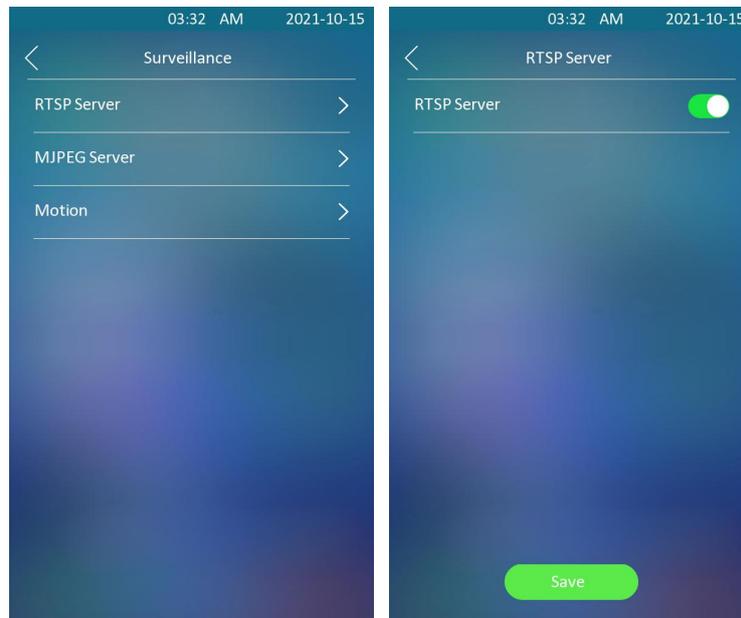
Enabled	<input checked="" type="checkbox"/>
Authorization Enabled	<input type="checkbox"/>
Authorization Mode	Digest
Username	admin
Password

Parameter Set-up:

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

- **User Name:** enter the name used for RTSP authorization.
- **Password:** enter the password for RTSP authorization.

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



14.3.2. 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 bit-rate etc. based on your actual network environment. Path: **Surveillance > RTSP > H.264 Video Parameters**.

H.264 Video Parameters

Video Resolution	1080P
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", "1080P". The default video resolution is "720P" and the video from the door phone might not be able to be shown in 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", "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 default if you want to obtained cropped video image and select Original if you want to obtain original video image.

**Note:**

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

14.4. ONVIF

Real-time video from the E18 camera can be searched and obtained by the Akuvox indoor monitor or by the third party devices such as NVR (**Network Video Recorder**) you can configure the ONVIF function in the door phone so that other device will be able to see the video from the door phone. Path: **Surveillance > ONVIF > Basic Setting**.

Surveillance >> ONVIF

Basic Setting

Discoverable	<input checked="" type="checkbox"/>
Username	<input type="text" value="admin"/>
Password	<input type="text" value="....."/>

Parameter Set-up:

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

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

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

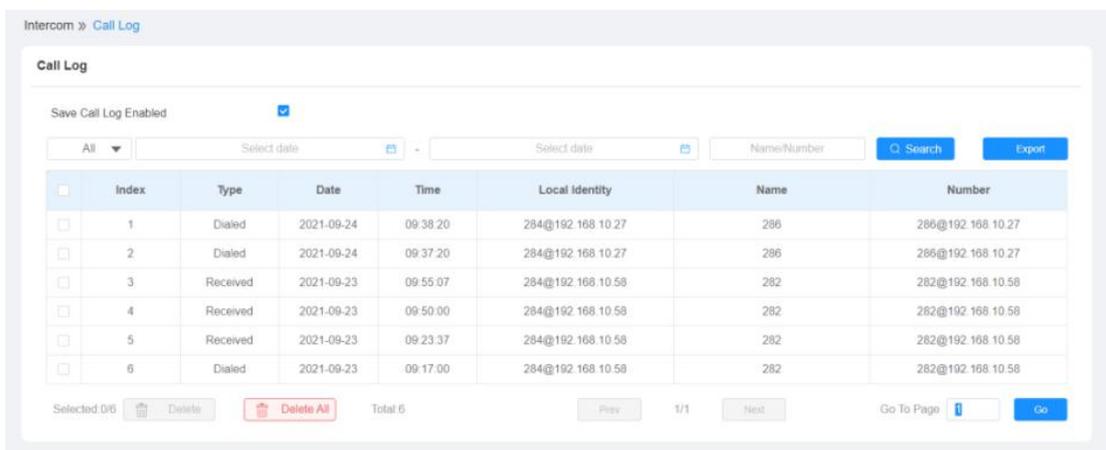
**Note:**

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

15. Logs

15.1. 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. Path:**Intercom > Call Log**



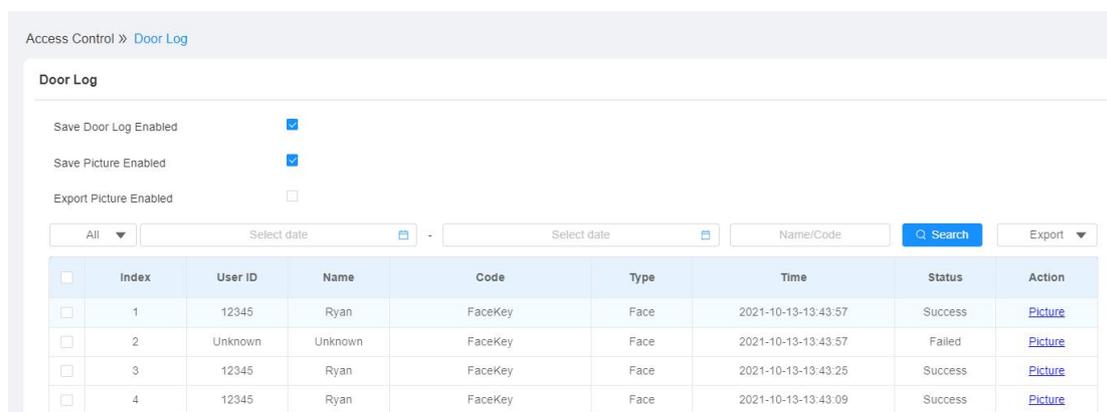
Parameter Set-up:

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

15.2.Door Logs

If you want to search and check on door access history, you can search and

check the door logs on the device web interface. Path: **Access Control > Door Log**.

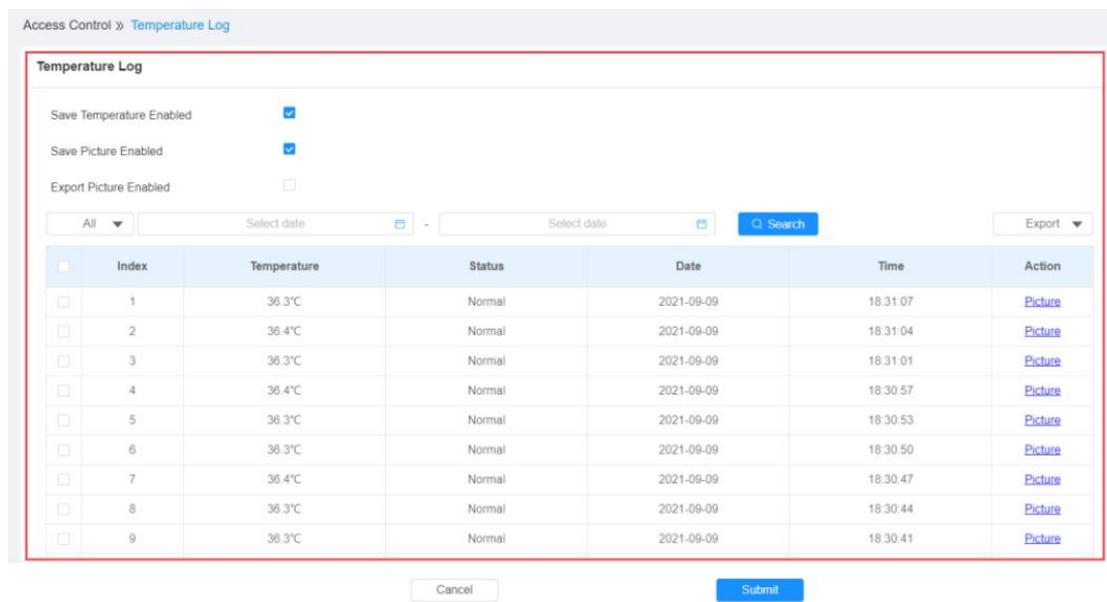


Parameter Set-up:

- **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 export the door log with 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 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.

15.3. Temperature Log

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

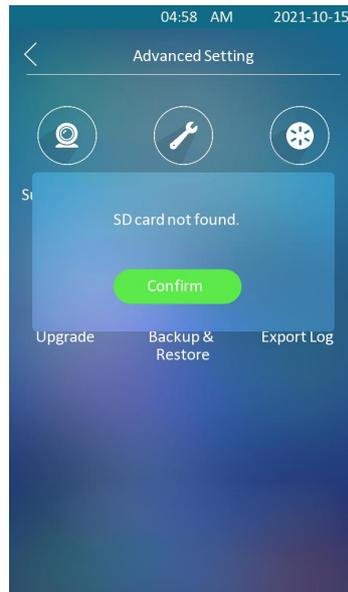


Parameter Set-up:

- **Save Door Log 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 export the temperature log with snapshot picture captured.
- **Time:** select the specific time select the specific time span of the temperature log you want to search, check or export.
- **Action:** click to display the picture captured.

15.4. Export Logs

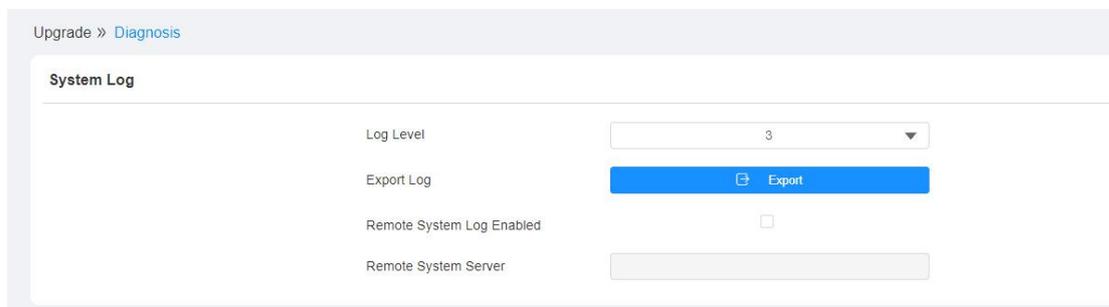
You can export door logs, call logs and temperature logs if needed. Path: **Advanced > Export Log.**



16. Debug

16.1. System Log for Debugging

System log in the door phone can be used for debugging purpose. 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 interface. Path: **Upgrade >Diagnosis > System Log.**



The screenshot shows the 'System Log' configuration page. At the top, there is a breadcrumb trail: 'Upgrade > Diagnosis'. Below this, the page title is 'System Log'. The configuration area contains four items: 'Log Level' with a dropdown menu set to '3'; 'Export Log' with a blue button labeled 'Export' and a download icon; 'Remote System Log Enabled' with an unchecked checkbox; and 'Remote System Server' with an empty text input field.

Parameter Set-up:

- **LogLevel:** 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 purpose. The default log level is "3", the higher the level is "5", the more complete the log is "7".
- **Export Log:** click the **Export** tab to export temporary debug log file to a local PC.
- **Remote System Log Enabled:** tick the checkbox to enable the function.
- **Remote System Server:** enter the remote server address to receive the the device log. And the remote server address will be provide by Akuvox technical support.

16.2.PCAP for Debugging

PCAP in E18 is used to capture the data package going in and out of the devices for debugging and troubleshooting purpose. You can set up the PCAP on the device web interface properly before using it. Path: **Upgrade >Diagnosis > PCAP.**

The screenshot shows the PCAP configuration page. At the top, it says 'PCAP'. Below that, there are three rows of controls:

- 'Specific Port' with a text input field containing '1~65535'.
- 'PCAP' with three buttons: 'Start' (blue), 'Stop' (grey), and 'Export' (blue).
- 'PCAP Auto Refresh' with a dropdown menu currently showing 'Disabled'.

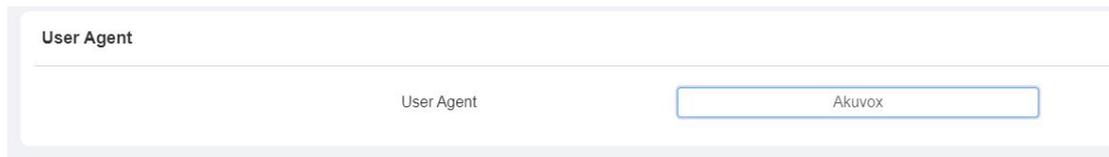
Parameter Set-up:

- **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:** click **Start** tab and **Stop** tab to capture the a certain range of data packets before clicking **Export** tab to export the data packets to you 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 packet even after the data packets reached its 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.

16.3.User Agent

SIP user agent (UA) is an endpoint device that supports SIP, which is used to establish connections an enable session 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 response. UA

acts as a SIP service provider for the specific user (device). You can customize user agent field in the SIP message. If user agent is set to specific value, users can see the information from PCAP. If 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.



User Agent

User Agent

Akuvox

Parameter Set-up:

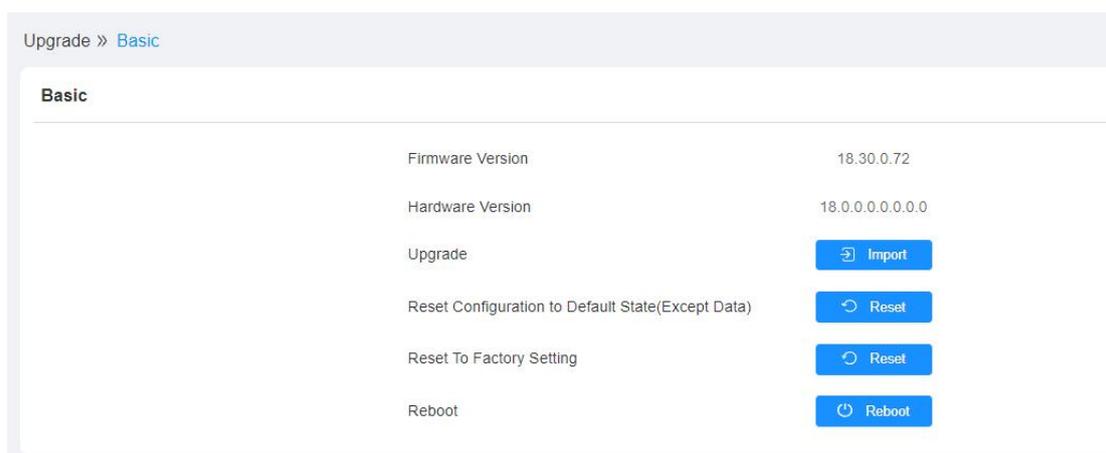
- **User Agent:** support to enter another specific value, Akuvox is by default.

17. Firmware Upgrade

E18 can be upgraded on the device and on the device web interface.

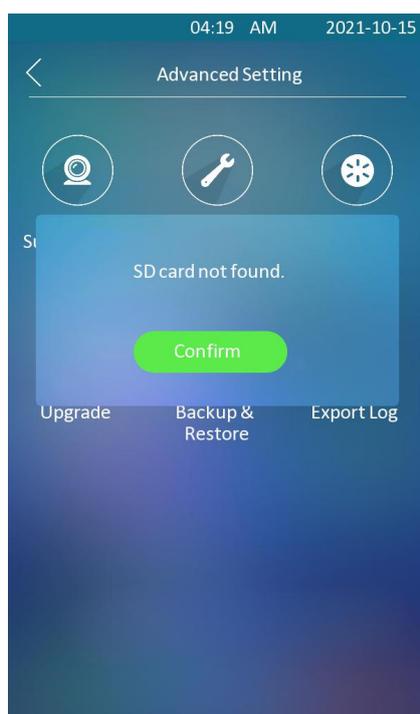
- Upgrade the device on the web interface

Path: **Upgrade > Basic.**



- Upgrade the device on the device

Path: **Advanced > Upgrade.**



**Note:**

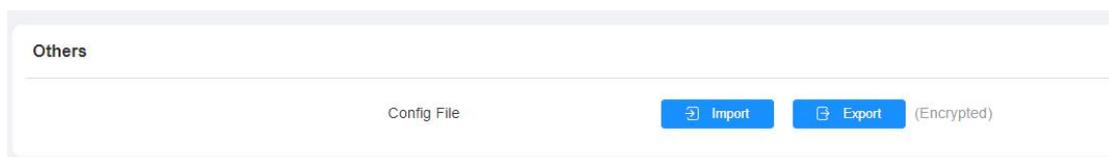
- When you insert the SD card, you are required to add a .rom file at the root directory and change the file name to update.com.

18. Backup

Configuration files and device data can be imported to or exported out of the device to your local PC on the device web interface if needed.

- Back up data on the web interface

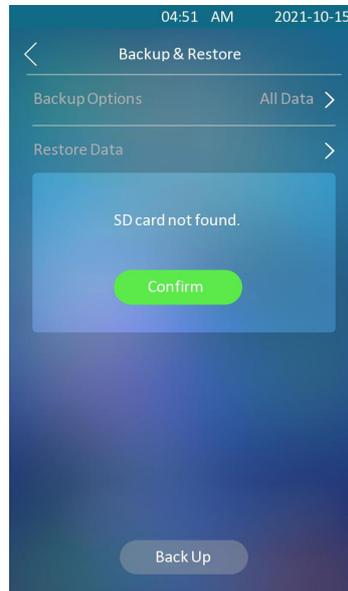
Path: **Upgrade > Diagnosis > Others**



- Back up data on the device

You need to insert the SD card to the device for the backup.

Path: **Advanced > Backup&Restore**



Parameter Set-up:

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

**Note:**

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

19. Auto-provisioning

Configurations and upgrading on E18 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 configuration needed one by one manually on the door phone.

19.1. Configuration Files for Auto-provisioning

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

The difference between the two types of configuration files is shown as 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 : r000000000018.cfg.
- **MAC-based configuration provisioning:** MAC-based configuration files is used for the auto-provisioning on a specific device as distinguished by its unique MAC number. And the configuration files named with 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.

19.2.AutoP Schedule

Akuvox provides you with different Autop methods that enable the door phone to perform provisioning for itself in a specific time according to your schedule. Path: **Upgrade > Advanced > Automatic Autop**.

The screenshot shows the 'Automatic Autop' configuration page. It features a 'Mode' dropdown menu currently set to 'Power On' and a 'Schedule' dropdown menu set to 'Sunday'. Below the schedule dropdown, there are two input fields: one for the hour (set to '22') with a '(0-23Hour)' label, and another for the minute (set to '0') with a '(0-59Min)' label. At the bottom of the form, there are two buttons: 'Clear MD5' with a trash icon and 'Export Autop Template' with a document icon.

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

19.3.PNP Configuration

Plug and Play (PNP) is a combination of hardware and software support that enables a computer system to recognize and adapt to hardware configuration changes with little or no intervention by a user. Path: configuration on web **Upgrade > Advanced > PNP Option** .

Upgrade » [Advanced](#)

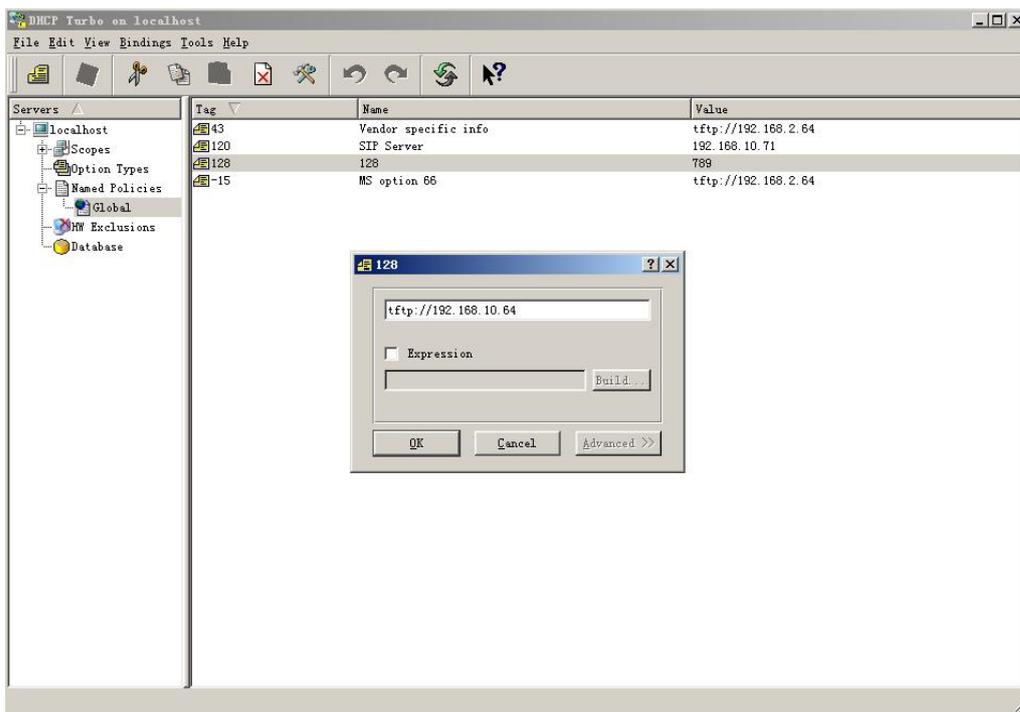
PNP Option

PNP Config Enabled



19.4.DHCP Provisioning Configuration

Auto-provisioning URL can also be obtained using DHCP option which allows 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 range from 128-255), you are required to configure DHCP Custom Option on the web interface. Path: **Upgrade > Advanced > DHCP Option**.



Note:

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



Note:

- The general configuration file for the in-batch provisioning is with the format "r0000000000xx.cfg" taking E18 as an example "r000000000915.cfg (10 "zeros" in total while the MAC-based configuration file for the specific device provisioning is with the format" MAC Address of the device.cfg, for example "0C110504AE5B.cfg."

19.5.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. Path:**Upgrade > Advanced > Automatic Autop.**

Manual Autop

URL	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>
Common AES Key	<input type="password"/>
AES Key(MAC)	<input type="password"/>

Parameter set-up:

- **URL:** set up tftp, http, https, ftp server address for the provisioning.
- **User Name:** set up a user name if the server needs an user name to be accessed to otherwise leave it blank.
- **Password:** set up a password if the server needs a password to be accessed to otherwise leave it blank.
- **Common AES Key:** set up AES code for the intercom to decipher general Auto Provisioning configuration file.
- **AES Key (MAC):** set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

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)

**Tip:**

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

20. Integration with Third Party Device

20.1. Integration via Wiegand

The door phone Wiegand interface is used to connect the door phone to the third party devices for the data transmission via weigand protocol. If you want to integrate the E18C door phone with the third party devices via Wiegand, you can configure the Wiegand on the web interface. Path: **Device > Wiegand > Wiegand**.

Parameter set-up:

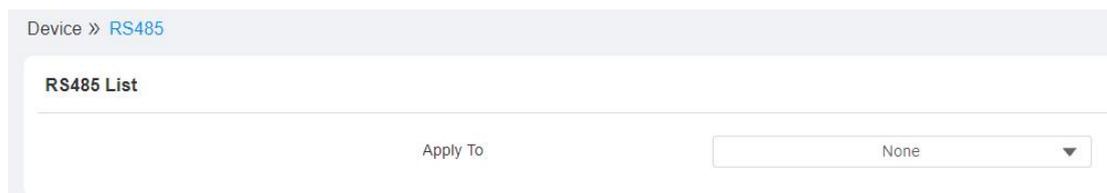
- **Wiegand Display Mode:** select Wigand Card code format among 8H10D; 6H3D5D; 6H8D; 8HN; 8HR; RAW.
- **Wiegand Card Reader Mode:** set the wiegand data transmission format among three options: " Wiegand 26", " Wiegand 34", " Wiegand 58". The transmission format should be identical between the door phone and the device to be integrated.
- **Wiegand 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 an vice versa.
- **Wiegand Output Data Order:** set the Wiegand output data sequence

between " Normal" and "Reversed" if you select " Reversed" then the input card number will be reversed an vice versa.

- **Wiegand Output CRC:** Tick to enable the parity check function to ensure that signal-based data can be transmitted correctly according to the established data transmission format.

20.2. Integration via RS485

RS485 is a physical interface used for two way data transmission between the two device. And RS485 Integration mode should be configured properly on the door phone's web interface before you can implement the integration between the door phone and the third party devices. Path:**Device > RS485 > RS485 List**.



Parameter Set-up:

- **RS485 List:** select integration mode between two options: " **None** " , " **OSDP** ", the detail for the two 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 E18 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 if that they use the same integration protocol.

20.3. OSDP Setting

OSDP (Open Supervised Device Protocol) is standard for access control communications designed to achieve two way communication among the devices over networks.

If you choose OSDP integration mode, you can not only check for OSDP status but also obtain the authentication from the third party devices for various applications such as door access etc. Path:**Device > RS485 > OSDP Advance Setting.**

The screenshot shows a web interface titled "OSDP Advanced Setting". It contains two main fields: "Connect Status" which is set to "Disconnected", and "Output With" which is a dropdown menu currently showing "OSDP".

Parameter Set-up:

- **Connect Status:** indicate OSDP based communication status.
- **Send by:** select in what way you want to send out the card number among three options: **"OSDP"**, **"Wiegand"** and **"None"**. if you select **"OSDP"** then the card number will be sent out to the third party devices via RS485. if you select **"Wiegand"** then the card number will be sent out via wiegand. If you select **"None"** then the card number will not be sent out but retained in the system.



Note:

- Dummy card numbers can not be sent if **"OSDP"** is not selected in the RS485 list field.

20.4.Integration via HTTP API

HTTP API is designed to achieve an network-based integration between the third party device with the Akuvox intercom device. You can configure the

HTTP API function on the web interface. Path: **Security > HTTP API**.

Security >> HTTP API

HTTP API

HTTP API Enable	<input checked="" type="checkbox"/>
Authorization Mode	<input type="text" value="Allowlist"/>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>
1st IP	<input type="text"/>
2nd IP	<input type="text"/>
3rd IP	<input type="text"/>
4th IP	<input type="text"/>
5th IP	<input type="text"/>

Parameter Set-up:

- **HTTP API Enable** enable or disable the HTTP API function for the third party integration. For example, if the function is disabled any request to initiate the integration will be denied and be returned HTTP 403 forbidden status.
- **Authorization Mode:** select among four options: **“None”** **“ WhiteList”** **“ Basic”**, **“ 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”**.
- **1st IP- 5th IP:** enter the IP address of the third party devices when the **“WhiteList”** authorization is select for the integration.

Please refer to the following description for the Authentication mode

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

20.5. Power Output Control

E18 can serve as a power supply for the external relays. Path: **Access Control > Relay > 12V Power Output**.

12V Power Output

Relay ID	RelayB
12v Power Output Enabled	<input type="text" value="Disabled"/>
Timeout(Sec)	<input type="text" value="3"/>

Parameter Set-up:

- **Relay ID:** Select the relay to be powered by E18.
- **12V Power Output:** select **Disabled** to disable the power output function; select **Always** to enable the access controller to provide continuous power to the third party device. Select **Triggered By Open Relay** if you want the E18 to provide power to the third party device via 12 output and GND interface during the timeout when the relays status is shifted from low to high.
- **Time Out (Sec):** select the the power supply time duration after the relay is triggered. Three options: 3, 5, 10. It is 3 seconds by default. The power output is 12V , and the maximum output amperage is 0.8A.

21. Password Modification

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

- Set and change web interface login password.

Path: **Security > Basic > Web Password Modify.**

The screenshot shows the 'Web Password Modify' section of the device's web interface. It includes a breadcrumb trail 'Security > Basic' and a 'Web Password Modify' title. Below the title, there is a 'Username' dropdown menu set to 'admin' and a blue 'Change Password' button. A modal dialog titled 'Change Password' is open, displaying a warning: 'The password must be at least eight characters long and contains at least one uppercase letter, one lowercase letter, and one digit.' The dialog contains four input fields: 'Username' (pre-filled with 'admin'), 'Old Password', 'New Password', and 'Confirm Password'. At the bottom of the dialog are 'Cancel' and 'Change' buttons.

- Set and change system PIN code.

Path: **Security > Basic > Web Password Modify.**

The screenshot shows the 'System PIN' section of the device's web interface. It features a 'System PIN' title and a 'PIN Code' input field with a masked password (dots).

22. System Reboot&Reset

22.1.Reboot

If you want to restart the device, you can operate it on the device web interface as well. More over, you can set up schedule for the device to be restarted. Path: **Upgrade > Basic**

Upgrade » Basic

Basic

Firmware Version	18.30.0.72
Hardware Version	18.0.0.0.0.0.0.0
Upgrade	Import
Reset Configuration to Default State(Except Data)	Reset
Reset To Factory Setting	Reset
Reboot	Reboot

To set up the device restart schedule, you can go to : **Upgrade > Advanced > Reboot Schedule.**

Reboot Schedule

Mode

Schedule

(0-23Hour)

Reboot Schedule

Mode	<input type="text" value="Disabled"/>
Schedule	<input type="text" value="Every Day"/>
Hour	<input type="text" value="0"/>
<input type="button" value="Submit"/> <input style="margin-left: 100px;" type="button" value="Cancel"/>	

22.2.Reset

You can reset the device to the factor setting and reset the device configuration to the default configuration setting on the device and on the device web interface.

➤ **To Reset the device on the device web interface**

Path: **Upgrade > Basic**

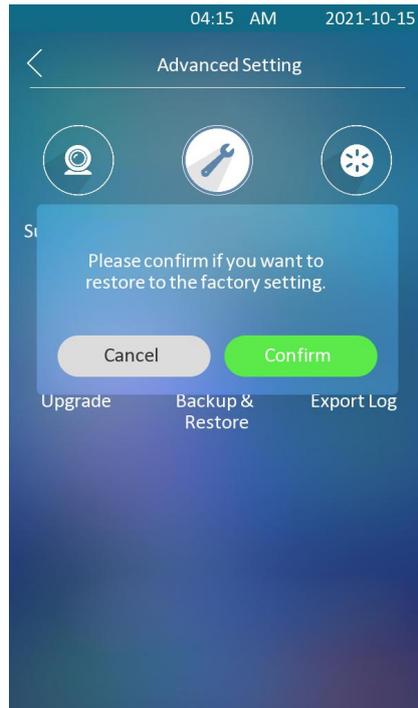
Upgrade » [Basic](#)

Basic

Firmware Version	18.30.0.72
Hardware Version	18.0.0.0.0.0.0.0
Upgrade	<input type="button" value="Import"/>
Reset Configuration to Default State(Except Data)	<input type="button" value="Reset"/>
Reset To Factory Setting	<input type="button" value="Reset"/>
Reboot	<input type="button" value="Reboot"/>

➤ **To Reset the device on the device**

Path: **Advanced > Reset.**



23. 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 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

SMTP: Simple Mail Transfer Protocol

SDMC: SIP Devices Management Center

TR069: Technical Report069

TCP: Transmission Control Protocol

TLS: Transport Layer Security

TFTP: Trivial File Transfer Protocol

UDP: User Datagram Protocol

URL: Uniform Resource Locator

VLAN: Virtual Local Area Network

WG: Wiegand

24. FAQ

Q1: How to obtain IP address of R2X

A1: ✓ For devices with single button - E21/ R20/ R23/ R26:

While E21/ R20/ R23/ R26 power up normally, hold the call button for 5 seconds after the statue LED turns blue and it will enter into IP announcement mode. In announcement mode, the IP address will be announced repeatedly. Press call button again to quit the announcement mode.

✓ For devices with multiple numeric keyboard - R27:

While R27 power up normally, press "*2396#" to enter home screen and press "1" to go to system Information screen to check the IP address.

✓ For devices with touch screen - R29:

While R29 power up normally, in the dial interface, press "9999", "Dial key", "3888" and "OK" to enter the system setting screen. Go to info screen to check the IP address.

✓ Common method:

Using Akuvox IP Scanner to search Akuvox devices in the same LAN network.

Q2: Do Akuvox devices support opus codec?

A2: For now, only Akuvox Android video IP phone R48G can support Opus audio codec.

Q3: What is the supported temperature range for akuvox doorphone?

A3: R20/E21/R26/R23/Standard R27/Standard R29 -- 14° to 112°F (-10° to 45°C)

R27/R29 with heating supporting --- 40 degrees

R28 -- (-40°C~55°C)

Indoorphone -- 14° to 112°F (-10° to 45°C)

IPPhone -- 32°~104°F(0~40°C)

Q4: Do Akuvox devices support Modbus protocol?

A4: No.

Q5: Failure in importing the R29 face data to another R29 using the exported face data .

A5: Please confirm the following steps:

The import format is zip;

1. After you export , you need to unzip the .tgz folder , then make the unzipped folder into .zip again.

Q55: Which version of ONVIF does R20 and R29 support?

A55: Onvif 18.04 profiles

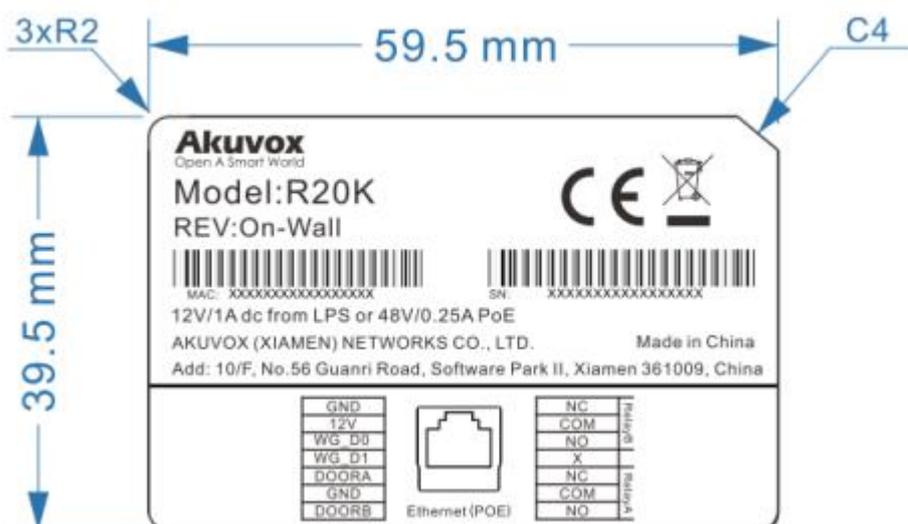
Q6: Do door phones support these card types? Prox, Legacy iClass,iClassSE,HID Mifare, HID DESFire,HID SEOS

A6: Sorry, they are not supported. They need to be implemented via hardware modifications.

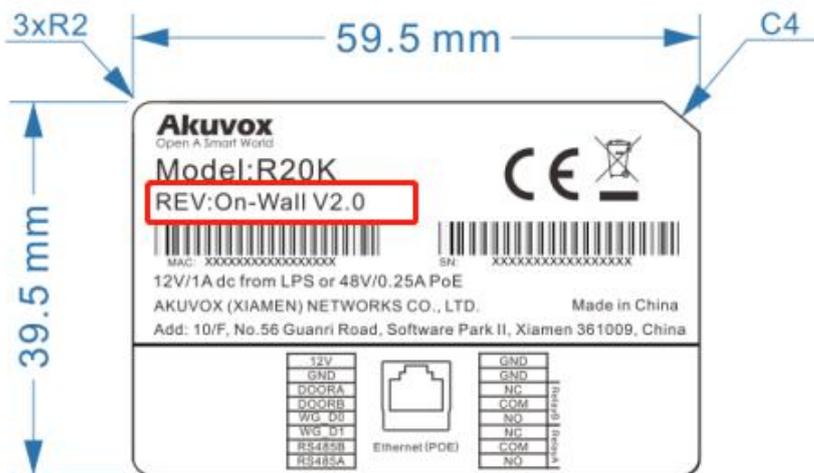
Q7: How to confirm whether my device is hardware version 1 or hardware version 2?

A7: 1.Label

● **Hardware version 1**



● **Hardware version 2**

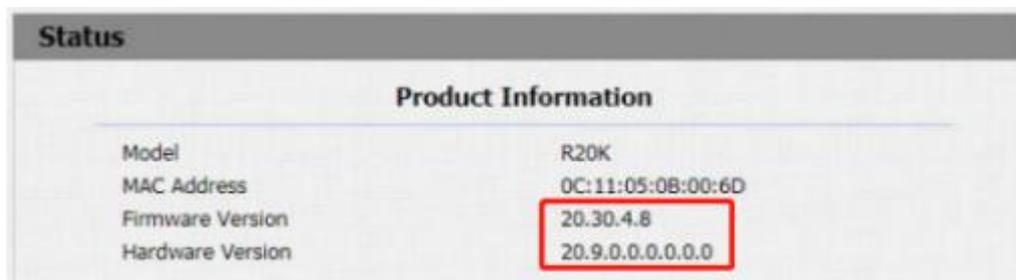


● **Firmware Version**

The firmware is different between hardware version1 and hardware version 2.
Go to Web-Status -Firmware Version.
20.X.X.X is hardware version 1.
220.X.X.X is hardware version 2.

● **Hardware version**

The firmware is different between hardware version1 and hardware version 2.
Go to Web-Status -Firmware Version.
If the hardware version is 220.x, then the device is hardware version 2.



25. 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.