



E16 SERIES DOOR PHONE

Administrator Guide

Version: 1.0 | Date: Jan.2021

About This Manual

Thank you for choosing Akuvox E16 series door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to 116.30.0.43 version, and it provides all the configurations for the functions and features of E16 series door phones. Please visit Akuvox forum or consult technical support for any new information or the latest firmwares.

Introduction of Icons and Symbols



Warning:



Caution:



Note:



Tip:

Related Documentation

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

<http://wiki.akuvox.com>

Table of Contents

1. Product Overview.....	1
2. Change Log.....	2
3. Model Specification.....	3
4. Installation.....	5
5. Introduction to Configuration Menu.....	17
6. Access the Device.....	20
6.1. Access the Device Setting on the device.....	21
6.2. Access the Device Setting on the Web Interface.....	22
7. Time and Language Setting.....	25
7.1. Language Setting.....	25
7.2. Time Setting.....	26
7.3. LED Setting.....	29
7.3.1. Configure Card Reader LED Setting.....	29
7.3.2. Configure LED White Light Setting.....	30
7.4. Screen Display configuration.....	32

7.4.1. Configure Screensaver.....	32
7.4.2. Upload Screensaver.....	34
7.5. Volume & Tone Configuration.....	37
7.5.1. Volume Configuration.....	37
7.5.2. Upload Open Door Tone.....	38
7.5.3. Configure Door Access Prompt Text.....	40
8. Network Setting.....	42
8.1. Device Network Connection Setting.....	42
8.2. Device Deployment in Network.....	44
8.3. NAT Setting.....	47
9. Intercom Call Configuration.....	48
9.1. IP call & IP Call Configuration.....	49
9.1.1. Make IP calls.....	49
9.1.2. IP Call Configuration.....	50
9.2. SIP Call & SIP Call Configuration.....	52
9.2.1. SIP Account Registration.....	52
9.2.2. SIP Server Configuration.....	54
9.2.3. Configure Outbound Proxy Server.....	56
9.2.4. Configure Data Transmission Type.....	58
9.3. Call Auto-answer Configuration.....	59
9.4. Call Settings.....	61

9.4.1. Maximum Call Duration Setting.....	61
9.4.2. Maximum Dial Duration Setting.....	63
9.4.3. Audio& Video Codec Configuration for SIP Calls.....	64
9.4.3.1. Configure Audio Codec.....	65
9.4.3.2. Configure Video Codec.....	66
9.5. Configure DTMF Data Transmission.....	68
10. Relay Switch Setting.....	70
10.1. Relay Switch Setting.....	70
10.2. Web Relay Setting.....	73
10.2.1. Configure Web Relay on the Web Interface.....	73
10.2.2. Configure Web Relay on the Device.....	77
11. Door Access Schedule Management.....	79
11.1. Configure Door Access Schedule.....	80
11.1.1. Create Door Access Schedule.....	80
11.1.2. Import and Export Door Access Schedule.....	83
11.1.3. Edit the Door Access Schedule.....	84
12. Door Unlock Configuration.....	85
12.1. Configure PIN Code for Door Unlock.....	86
12.1.1. Configur Public PIN code.....	86
12.1.2. Configure Private PIN Code on the Device.....	88
12.1.3. Configure Private PIN Code on the Web Interface.....	89

12.1.4. Configure Private PIN Access Mode.....	93
12.2. Configure RF Card for Door Unlock.....	95
12.2.1. Configure RF Card on the Web Interface.....	95
12.2.1.1. Configure RF Card Code Format.....	96
12.2.2. Configure Facial Recognition for Door Unlock.....	97
12.2.2.1. Configure Facial Recognition on the Device..	98
12.2.2.2. Configure Facial Recognition on Web Interface	99
12.3. Configure Door Access Using Configured Files.....	101
12.4. Editing the User(s)-specific door access data.....	103
12.4.1. Unlock by QR Code.....	104
12.4.2. Unlock by Bluetooth.....	105
12.4.3. Unlock by HTTP Command on Web Browser.....	107
12.4.4. Unlock by Exit Button by the Door.....	109
12.4.5. Unlock by Reception Tab.....	111
12.4.6. Unlock by DTMF Code.....	113
12.4.7. Body Temperature Measurement for Door Access (Optional)	115
12.4.7.1. Body Temperature Measurement Configuration	115
12.4.7.2. Ambient Temperature Configuration.....	118
13. Security.....	120
13.1. Tamper Alarm Setting.....	120

13.2. Motion Detection	122
13.3. Security Notification Setting	122
13.3.1. Email Notification Setting	122
13.3.2. FTP Notification setting	124
13.3.3. TFTP Notification Setting	126
13.4. Web Interface Automatic Log-out	127
14. Monitor and Image	128
14.1. Mjpeg Image Capturing	128
14.2. Live Stream	130
14.3. RTSP Stream Monitoring	132
14.3.1. RTSP Basic Setting	132
14.3.2. RTSP Stream Setting	134
14.4. ONVIF	137
15. Logs	140
15.1. Call Logs	140
15.2. Door Logs	141
15.3. Temperature Log	143
16. Debug	145
16.1. System Log for Debugging	145
16.2. PCAP for Debugging	147
17. Firmware Upgrade	150

18. Backup	151
19. Auto-provisioning via Configuration File	153
19.1. Provisioning Principle	153
19.2. Configuration Files for Auto-provisioning	154
19.3. AutoP Schedule	156
19.4. DHCP Provisioning Configuration	158
19.5. Static Provisioning Configuration	162
20. Integration with Third Party Device	166
20.1. Integration via Wiegand	167
20.2. Integration via RS485	169
20.3. OSDP Setting	171
21. Password Modification	173
22. System Reboot&Reset	175
22.1. Reboot	175
22.2. Reset	177
23. Abbreviations	178
24. FAQ	182
25. Contact Us	187


1. Product Overview

Akuvox E16 series is an Android-based IP video door phone with a touch screen. It incorporates audio and video communications, access control, and video surveillance. Its finely-tuned Android OS, SmartPlus and AI-based communication technology allow featured customization to better suit your operation habit. E16 series 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. E16 series 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




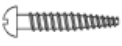
	E16C
Model & Feature	
Display	5" IPS
Touch Screen	√
Button	X
Housing Material	Plastic
Relay Out	1
Alarm In	1
RS485	√
PoE	√
Resolution	1280x720
Brightness	500cd/m ²
RAM	1GB
ROM	8GB

Wall Mounting	√
Flush Mounting	√
Desk Mounting	X
Wall Mounting Dimension	√
Wall Mounting Dimension	√
POE Stand by Power	5.5W





4. Installation

- Universal Accessories

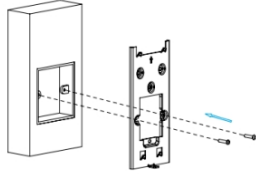
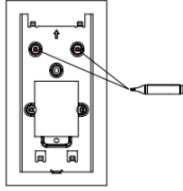
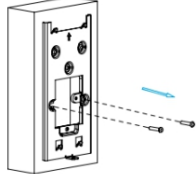
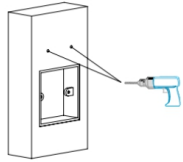
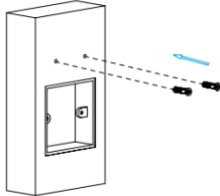

No.	Accessories	Description	Quantity
1		E16	1
2		Wall-mounting bracket	1
3		Cable locking plate	1
4		Back cover	1
5		Rubber Plug	3
6		Allen Wrench	1
7		Torx Wrench	1
8		Plastic Wall Anchor	4
9		M3x6 Screw	4
10		M4x30 Screw	2
11		Torx Screw	1

12	 	M2.5x6 Screw	2
13	 	ST4x20 Screw	4

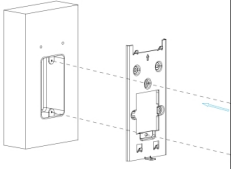
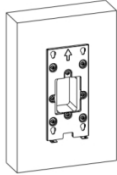
- *Digital Temperature Detector Accessories (Optional)*

No.	Accessories	Description	Quantity
1		Digital Forehead Temperature Detector	1
2		Digital Wrist Temperature Detector	1
3		M3x6 Screw	2
4		3x10.5 Screw	2

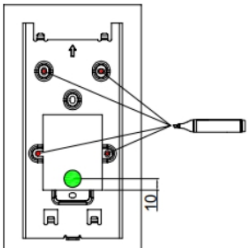
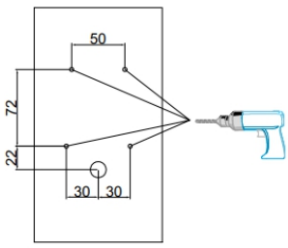
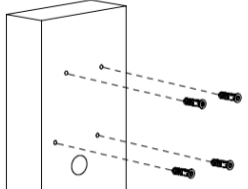
- Wall-mounting bracket installation with 86x86 mm embedded

Steps	Installation Picture	Installation Description
1		<p>Fix the wall-mounting bracket on the embedded box with two M4x30 screws.</p>
2		<p>Mark the two positioning holes of the wall-mounting bracket on the wall.</p>
3		<p>Remove the two M4x30 screws and take off the wall-mounting bracket.</p>
4		<p>Use a hand drill with 5mm diameter bit to make two positioning holes with 5mm in depth in the marked positions.</p>
5		<p>Insert two plastic wall anchors into the two drilled holes.</p>
		<p>Fix the wall-mounting bracket with</p>

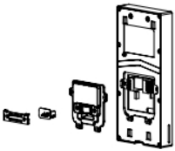
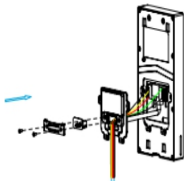
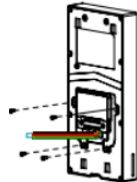
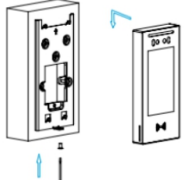
- With 2x3 Inches Embedded Single-gang Box in the Wall

Steps	Installation Picture	Installation Description
1		<p>Fix the wall-mounting bracket on the single-gang junction box with the two M4x30 screws.</p>
2		<p>Finish the bracket installation.</p>

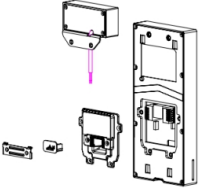
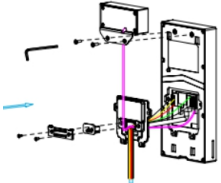
- With Embedded Gang box in the Wall

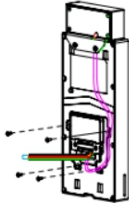
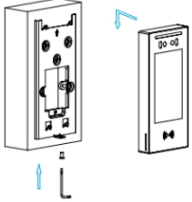
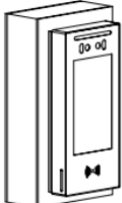
Steps	Installation Picture	Installation Description
1		<p>According to the position of the cable, put the wall-mounting bracket closely on to the wall and mark the four positioning holes, while making sure that relative positions between wall-mounting bracket and wire hole are correct.</p> <p><i>Note:</i> The positioning holes should be market in the center of the holes.</p>
2		<p>Take off the wall-mounting and drill the four marked positioning holes and the wire holes using 5mm hand drills.</p>
3		<p>Insert four plastic wall anchors into the holes.</p>

- *Device Installation without Digital Temperature Detector*

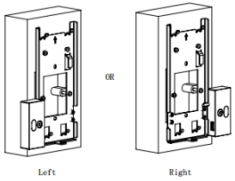
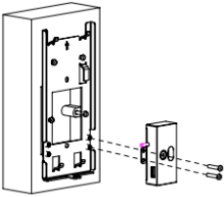
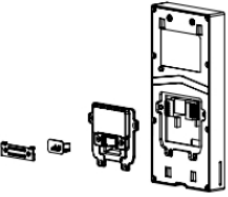
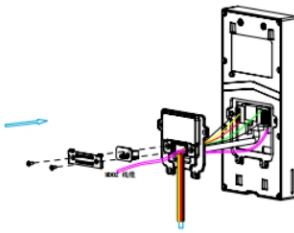
Step s	Installation Picture	Installation Description
1		<p>Take out the device along with the back cover, cable locking plate , rubber plug and corresponding screws.</p>
2		<p>Lead the wires from the wall-mount bracket and the module through the square hole on the back cover, connecting them to the corresponding interface of the main board.</p> <p>Select a suitable size rubber plug to push all the cables into the back cover. Fix cable locking plate to the back cover with two M2.5x6 screws using the Allen wrench attached with.</p>
3		<p>Fasten the back cover with four M3x6 screws using the Allen wrench attached with.</p>
4		<p>Hang the device on to the square hanger on the wall mounting bracket, pull down the device to make it fall completely on to the square hanger on</p>

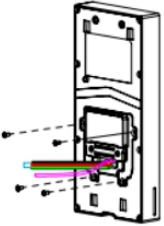
● *Device Installation with Digital Forehead Temperature Detector*

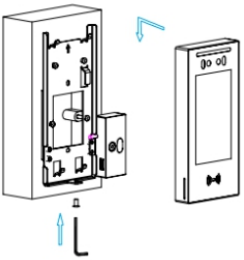
<i>Steps</i>	<i>Installation Picture</i>	<i>Installation Description</i>
1		<p><i>Take out the door phone and the digital forehead temperature detector and then take out back cover, cable locking plate and rubber plug.</i></p>
2		<p><i>Fasten the detector on to the nuts on the device's rear cover with two M3X10.5 screws using the Allen wrench attached with, and lead the wires from the wall-mount bracket and the detector through the square hole on the back cover, connecting them to the corresponding interface of the main board. And then select a suitable size rubber plug to push all the cables into the back cover. Fix cable locking plate to the back cover with two M2.5x6 screws using the Allen wrench attached with.</i></p>

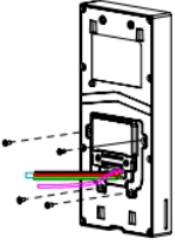
<p>3</p>		<p>Fasten the back cover with four M3x6 screws using the Allen wrench attached with.</p>
<p>4</p>		<p>Hang the device on to the square hanger on the wall mounting bracket, pull down the device to make it fall completely on to the square hanger on the wall-mounting bracket, then use the Torx Wrench attached with to tighten the device with the Torx screw.</p>
<p>5</p>		<p>Installation is completed.</p>

● *Device Installation with Digital Wrist Temperature Detector*

Step s	Installation Picture	Installation Description
1		<p>Fix the the two holes of the detector onto the installation pins on the wall-bracket either on the left or right according to your preference.</p>
2		<p>Tighten the detector on to the inner threaded bolt with two M3x6 screw using the Allen wrench attached with in the same on both side.</p>
3		<p>Take out the device along with the back cover, cable locking plate , rubber plug and corresponding screws.</p>
4		<p>Fasten the module on to the nuts on the device' s rear cover with two M3X6 screws using the Allen wrench attached with, then Lead the wires from the wall-mount bracket and the module through the square hole on the back</p>

		<p>cover, connecting them to the corresponding interface of the main board. And then Select a suitable size rubber plug to push all the cables into the back cover. Fix cable locking plate to the back cover with two M2.5x6 .</p>
<p>5</p>		<p>Fasten the back cover with four M2.5x6 screws.</p>

<p>6</p>		<p>Hang the device on to the square hanger on the wall mounting bracket, pull down the device to make it fall completely on to the square hanger on the wall-mounting bracket, then use the Allen Wrench attached with to tighten the device with two M3x6 screws.</p>
----------	-------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7	 A technical diagram of the back cover of the Akuvox E16X intercom. The cover is shown in a perspective view, with four screws being inserted into pre-drilled holes. Dashed lines indicate the alignment of the screws. A small Allen wrench is shown at the bottom left, with a colored handle (red, yellow, green, blue) and a silver tip, positioned to tighten one of the screws.	<p><i>Fasten the back cover with four M2.5x6 screws using the Allen wrench attached with.</i></p>
---	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------

5. 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.

- *Setting: this second deals with time & language setting, security notification settings and door prompt text setting.*
- *Phone: this section includes Time&language, call feature, dial management, data import&export, door log, web relay.*
- *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.*
- *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.*

- *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.

6. Access the Device

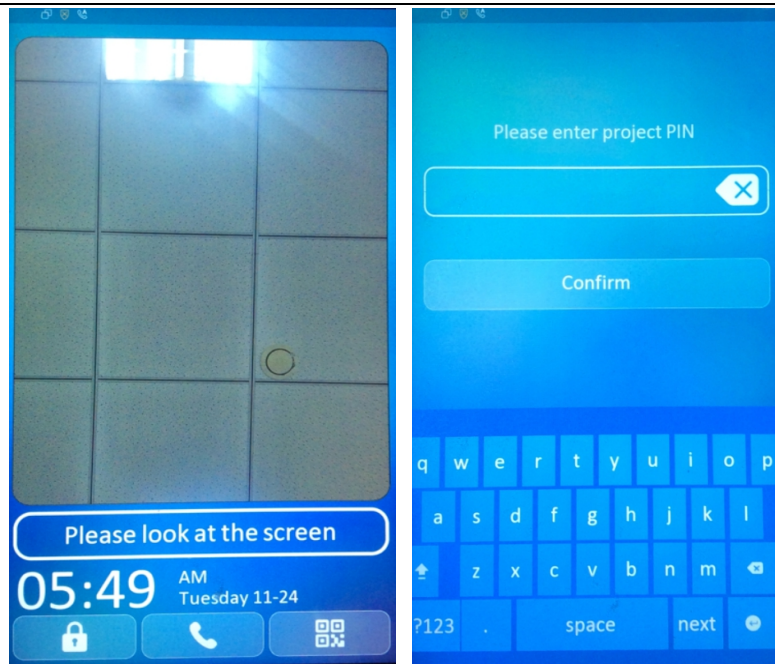
E16 series door phone system setting can be either accessed on the device directly or on the device web interface.

6.1. Access the Device Setting on the device

If you want to access the device setting in order to configure and adjust the parameters, you can do it directly on the device.

To access the device setting, you can do as follows:

- 1. Long press any where on the initial screen for approximately five seconds to go to project PIN screen.*
- 2. Enter the default PIN code “admin”.*
- 3. press **Confirm** tab to go to Setting screen.*



6.2. Access the Device Setting on the Web Interface

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

To log in device web interface, you can do as follows:



1. Press the **Info** icon on the Setting screen.
2. Check the device IP address on the device.
3. Enter the IP address on the web browser.
4. Enter the **User Name** and **Password** of the device web interface.
5. Click **Login** tab to log in the web interface.

A screenshot of the Akuvox web interface login page. The page has a dark blue header with the 'Akuvox' logo in white. Below the header is a white login form with a light blue border. The form contains three input fields: 'User Name' with a person icon, 'Password' with a lock icon, and a checkbox labeled 'Remember Username/Password'. At the bottom of the form is a blue 'Login' button with white text.

 **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 [IP Scanner](#) for more details.

 **Note:**

- Google Chrome browser is strongly recommended.

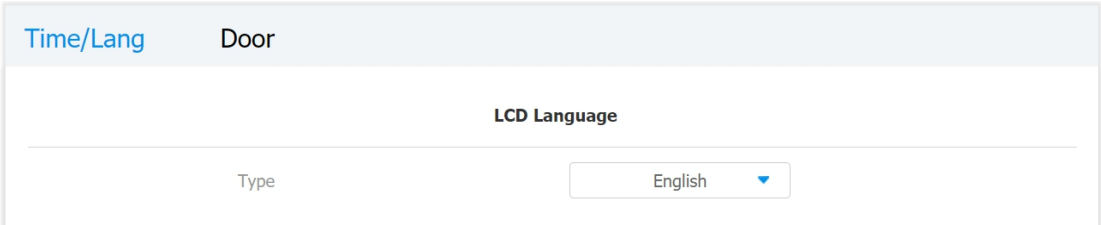
7. Time and Language Setting

7.1. Language Setting

When you first set up the device, you might need to set the language to your need. You can select the language display the device web interface.

To select the language, you can do as follows:

1. Click **Setting >Time/Lang > LCD Language**
2. Select the language you need and click **Submit** tab for validation.



The screenshot shows a web interface for configuring the LCD Language. At the top, there are two tabs: "Time/Lang" (which is selected and highlighted in blue) and "Door". Below the tabs, the page title is "LCD Language". There is a horizontal line separating the title from the content area. Below the line, there is a label "Type" and a dropdown menu. The dropdown menu is currently set to "English" and has a small blue triangle indicating it can be expanded.

7.2. Time Setting

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 so that the NTP server can synchronize the time zone setting in your device.

To configure the time setting on the web interface, you can do as follows:

1. Click *Setting >Time/Lang > Time*
2. Untick the check box to allow you to set the time and date manually.
3. Tick the check box to enable the NTP server function that allows you to synchronize your time setting via NTP server.
4. Enter the NTP server you obtained in the field of the primary and secondary NTP server.
5. Set up the update timing via NTP server.
6. Click the *Submit* tab for the validation and the *Cancel* tab for the cancellation.

Time

Enabled	<input type="checkbox"/>
Date	<input type="text" value="mm/dd/yyyy"/>
Time	<input type="text" value="--:-- --"/>
Time Zone	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">GMT-5:00 Toronto ▼</div>
Primary Server	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">0.pool.ntp.org</div>
Secondary Server	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">1.pool.ntp.org</div>
Update Interval	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">3600</div>

Submit

Cancel

Parameter Set-up:

- **Time Zone:** select the specific time zone depending on where the device is used and then press **Confirm** tab for the confirmation. The default time zone is GMT+0.00.
- **Primary Server:** enter the primary NTP server you obtained in the NTP Server field.
- **Secondary Server:** enter the secondary NTP server you obtained in the NTP Server field to be used as a backup.
- **Update Interval:** set the automatic time update via NTP server.

Note:

7.3. LED Setting

7.3.1. 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.

To do the configuration, you can do as follows:

1. Click **Device > Light > LED of Swiping Card Area**
2. Set the parameter and click **Submit** tab for the validation.

Light	Wiegand	RS485	Voice	LCD
LED Of Swiping Card Area				
Enabled		<input type="checkbox"/>		
Start Time - End Time		18	-	06 (0~23 Hour)

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).

7.3.2. 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.

To set up the white light function, you can do as follows:

1. Click *Device > Light > White Light*
2. Set up parameter properly.
3. Click *Submit* tab for the validation and *Cancel* tab for the cancellation.

White Light

Mode: Auto

Max White Light Value: 3

Submit Cancel

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

7.4. Screen Display configuration

E16 series 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.

7.4.1. Configure Screensaver

Await screen is mainly a function for the screen protection. 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.

Parameter set-up:

1. Click *Device > LCD > Standby Interface Display*
2. Set up parameters properly according to your need.
3. Click *Submit* tab for the validation and *Cancel* tab for the cancellation.

Standby Interface Display	
ScreenSaver Mode	<input checked="" type="checkbox"/>
Sleep	15seconds ▼
Screensaver Time	15seconds ▼

Parameter Set-up

- **ScreenSaver Mode:** tick the check box to enable the screen saver function.
- **Sleep:** set the screen saver start time range from “5” seconds to “30” minutes For example, if you set it as “15 seconds” then the device will go into screen saver mode in 15 second when when there is no operation on the device or no one is detected approaching

7.4.2. Upload Screensaver

You can upload screensaver pictures separately or in batch to the device and to the device web interface for publicity purpose or for a greater visual experience.

To do so, you can do as follows:

1. Click **Device > LCD > Upload ScreenSaver**
2. Click **Select File** tab to choose the picture you want to upload to the device.
3. Click **Import** tab to start uploading the pictures (5 pictures maximum in total)
4. Click to designate the ID order number to the picture uploaded from image 1 to image 5 in the **Please Choose ScreenSaverID-for upload** field.
5. Set the display time of each individual picture you uploaded in **Interval (Sec.)** the display time range is from "1-120" seconds.
6. Click **Submit** tab or **Delete** tab for the confirmation or the cancellation of the pictures uploaded with the designated ID order

number.

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.

Please see the picture below:

Upload ScreenSaver

Please Choose ScreenSaverID-for upload: Screen Saver1 ▾

Screen Saver1 Not selected any files Select File Import

ScreenSaver ID	File Status	Interval (Sec)	Delete
1	File Exists	<input type="text" value="5"/>	Delete
2	File Exists	<input type="text" value="5"/>	Delete
3	File Exists	<input type="text" value="5"/>	Delete
4	File Exists	<input type="text" value="5"/>	Delete
5	File Exists	<input type="text" value="5"/>	Delete

Submit Cancel



Note:

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

7.5. Volume & Tone Configuration

Volume and tone configuration in E16 door phone refers to the Call volume, the AD volume, key volume and Mic volume and open door tone configuration. Moreover, you can upload the tone you like to enrich your personalized user experience.

7.5.1. 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.

To set up the volumes on the device , you can do as follows:

1. Click Device > Voice > Volume Control
2. Set up volume and ringtone parameters according to your need.
3. Press Submit tab for the validation.

Light	Wiegand	RS485	Voice	LCD
Volume Control				
	Mic Volume	<input type="text" value="8"/>	(0~15)	
	Speaker Volume	<input type="text" value="8"/>	(0~15)	
	Ring Volume	<input type="text" value="8"/>	(0~15)	
	Tamper Alarm Volume	<input type="text" value="8"/>	(0~15)	

- **Mic Volume:** set the mic volume from 0-15 according to your need. The default volume is “8”.
- **Speaker Volume:** set the speaker volume from 0-15 according to your need. The default volume is “8”.
- **Ring Volume:** set the ring volume from 0-15 according to your need. The default volume is “8”.
- **Tamper Alarm Volume:** set the tamper alarm volume from 0-15 according to your need. The default volume is “8”.

7.5.2. Upload Open Door Tone

You can upload the Open Door Tone on the device web interface.

To upload open door tone, you can do as follows:

1. Click **Device > Voice > Open Door Tone Setting**
2. Tick the check box in **Open Door Tone Setting** field to enable the open door time setting.
3. Click **Select File** tab to upload the .wav files you selected to the device.
4. Click **Import** tab to import the .wav files.
5. Click **Reset** tab if you want to reset the file uploaded.
6. Click the **Submit** tab for the validation and **Cancel** tab for the cancellation.

The screenshot shows the 'Open Door Tone Setting' web interface. At the top, the title 'Open Door Tone Setting' is centered. Below the title, there is a checkbox labeled 'Open Door Tone Setting' which is checked. Underneath, there is a section for 'Open Door Tone Upload'. It features a text input field containing 'Not selected any files', followed by a 'Select File' button. To the right of this are three buttons: 'Import' (with a folder icon), 'Reset', and 'Submit'. At the bottom of the form, there are two buttons: 'Submit' and 'Cancel'.

7.5.3. *Configure Door Access Prompt Text*

You can enable or disable the door access prompt to be shown on the door phone screen for door open failure and success.

To do the configuration, you can do as follows:

- 1. Setting > Door > Open Door Succeeded Text Prompt*
- 2. Enable or disable the Prompt text for both open door failure and success.*
- 3. Press Submit tab for the validation and Cancel tab for the cancellation.*

Time/Lang	Door
Open Door Succeeded Text Prompt	
Open Door Succeeded Text Prompt	<input checked="" type="checkbox"/>
Open Door Failed Text Prompt	<input checked="" type="checkbox"/>
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

Parameter set-up:

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

8. Network Setting

8.1. 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, LAN DNS1 & LAN DNS2.

To configure the device network connection, you can do as follows:

1. Click *Network > Ethernet > LAN Port*
2. Select *DHCP mode* or *Static IP mode* by ticking off their respective check box.
3. Click *Submit* tab for the validation or *Cancel* tab for the cancellation.

Ethernet

LAN Port

DHCP Static IP

IP Address

Subnet Mask

Default Gateway

LAN DNS1

LAN DNS2

Parameter Set-up:

- **DHCP:** select the **DHCP** mode by checking off the **DHCP** box. **DHCP** mode is the default network connection. If the **DHCP** mode is selected, 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.*
- *DNS1/DNS2: set up DNS1/ DNS2 (Domain Name Server) according to your actual network environment. DNS1 is the primary DNS server address while the DNS2 is the secondary server address and the door phone connects to DNS2 server when the primary DNS server is unavailable .*

8.2. Device Deployment in Network

Door phones should be deployed before they can be properly configured in the network environment in terms of their location,

- **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 Address:** specify the device address by entering device location information from the left to the right :*Community*, *Unit*, *Stair*, *Floor*, *Room* in sequence.
- **Device extension:** enter the device extension number for the device you installed
- **Device Location:** enter the location in which the device is installed and used.

8.3. NAT Setting

In order to speed up the communication between the door phone and the SIP server, you can configure the NAT setting (Network Address Translation) on the web interface.

To set up NAT, you can do as follows:

1. Click **Account > Advanced > NAT**
2. Set parameters properly.
3. Click **Submit tab** for the validation and **Cancel tab** for the Cancellation.



The screenshot shows a web interface for NAT settings. At the top, the word "NAT" is centered. Below it, there is a horizontal line. Underneath the line, on the left, is the label "RPort". To the right of "RPort" is a dropdown menu with the text "Disabled" and a small downward-pointing triangle icon.

Parameter Set-up:

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

9. 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.

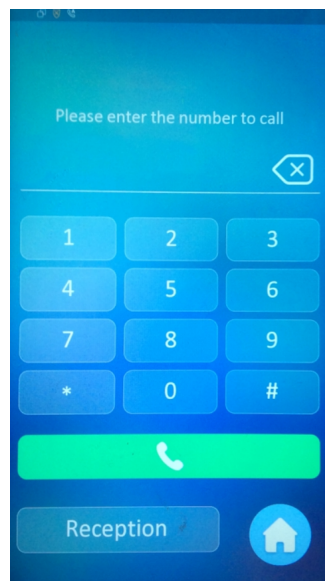
9.1. IP call & IP Call Configuration

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.

9.1.1. Make IP calls

To make directly IP call on the device, you can do as follows:

1. Press the dial  icon on the home screen to go to the Dial interface on the device.
2. Enter the IP or SIP number you wish to call on the soft key board.
3. Press the Call  icon to call out.



 **Note:**



9.1.2. IP Call Configuration

To configure the IP call on the device web interface, you can do as

follows:

1. Click *Intercom > Basic > Direct IP*
2. Set up related parameters as needed.
3. Click *Submit* tab for the validation or *Cancel* tab for the cancellation.

Basic Call Feature	
Direct IP	
Enabled	<input checked="" type="checkbox"/>
Port	<input type="text" value="5060"/> (1~65535)

Parameter set-up:

- *Direct IP Call:* click “**Enable**” or “**Disable**” to turn the direct IP call on or off. For example if you do not allow direct IP call to be made on the device, you can click” **Disable**” to terminate 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.

9.2. SIP Call & SIP Call Configuration

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.

9.2.1. SIP Account Registration

E16 series door phones support two SIP accounts that can all be registered according to your applications. The SIP account can be configured on the device interface.

To perform the SIP account setting on the Web Interface, you can do

as follows:

1. Click **Account > Basic > SIP Account**
2. Set up parameters for the SIP Account.
3. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.

Basic	Advanced
SIP Account	
Status	<input type="text" value="Disabled"/>
Account Active	<input style="border-bottom: 1px solid #ccc;" type="text" value="Disabled"/>
Display Label	<input type="text"/>
Display Name	<input type="text"/>
Register Name	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password" value="....."/>

Parameter Set-up:

- **Status:** check to see if the SIP account is registered or not.
- **Account Active:** click “Enable” or “Disable” to activate or

deactivate the registered SIP account.

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

9.2.2. SIP Server Configuration

SIP servers can be set up for device in order to achieve call session

through SIP server between intercom devices.

To set up SIP server , you can do as follows :

1. Click **Account > Basic > Preferred SIP Server**
2. Enter parameters required.
3. Press **Submit** tab for the validation and **Cancel** tab for the cancellation.

Preferred SIP Server			
Server IP	<input type="text"/>	Port	<input type="text" value="5060"/>
Registration Period	<input type="text" value="1800"/>		
Alternate SIP Server			
Server IP	<input type="text"/>	Port	<input type="text" value="5060"/>
Registration Period	<input type="text" value="1800"/>		

Parameter Set-up:

- **Preferred SIP Server:** enter the primary server IP address number or its URL.

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

9.2.3. *Configure Outbound Proxy Server*

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

To configure outbound Proxy server, you can do as follows:

1. *Click Account - Basic > Outbound Proxy Server*

2. Set up parameters properly.
3. Press **Submit** for the validation.

Outbound Proxy Server

Enable Outbound	<input type="text" value="Disabled"/>		
Server IP	<input type="text"/>	Port	<input type="text" value="5060"/>
Backup Server IP	<input type="text"/>	Port	<input type="text" value="5060"/>

Parameter Set-up:

- **Enable Outbound:** click “**Enable**” and “**Disable**” to turn on or turn off the outbound proxy server.
- **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
- **Backup 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

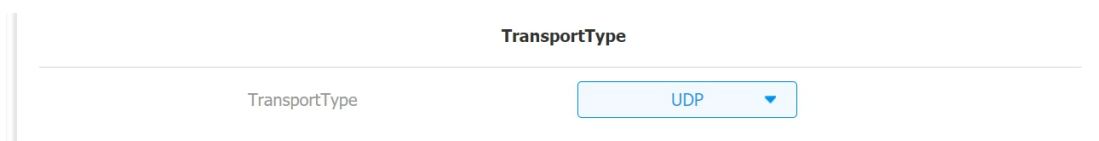
backup outbound proxy server.

9.2.4. 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.

To do the configuration , you can do as follows:

1. Click **Account > Basic > Transport Type**
2. Select the Transport type according to your need.
3. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.



The screenshot shows a configuration form for 'TransportType'. The form has a label 'TransportType' and a dropdown menu currently set to 'UDP'. The dropdown menu is highlighted with a blue border and a small downward arrow.

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.*

9.3. Call Auto-answer Configuration

You can define how quick the door phone should response in answering the incoming SIP/IP call automatically by setting up the time related parameters. In addition, you can also define the mode in which the calls are to be answered (video mode or audio mode)

To do the configuration, you can do as follows:

1. Click **Account > Advanced > Call**
2. Click “**Enable**” or “**Disable**” in **Auto Answer** field to turn on or turn off the Auto Answer function.
3. Set up auto-answer delay time.
4. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.
5. Click **Intercom > Call Feature > Auto Answer**
6. Click **Mode** to select “**Audio**” or “**Video**” auto-answer mode.
7. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.

Call	
Auto Answer	Disabled ▾
Auto Answer Delay	0

Auto Answer

Auto Answer Delay (0~5 Sec)

Mode ▼

Parameter Set-up:

- *Auto Answer: turn on the the Auto Answer function by clicking “Enable”.*

- *Auto Answer Delay: set up the delay time (from 0-5 sec.) before the call an 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.*

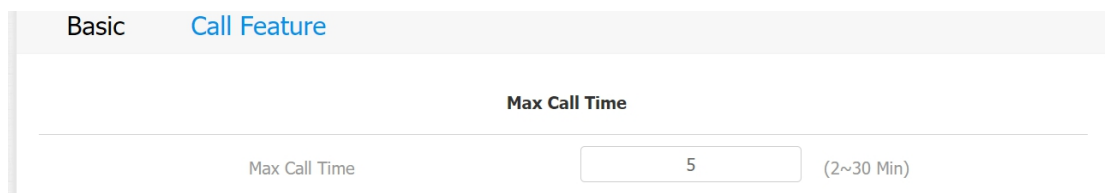
9.4. Call Settings

9.4.1. Maximum Call Duration Setting

E16 series 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.

To do the configuration, you can do as follow:

1. Click **Intercom > Call Feature > Max Call Time**
2. Enter the call time duration in in the **Max Call Time** field.



The screenshot shows a web interface with two tabs: 'Basic' and 'Call Feature'. The 'Call Feature' tab is active. Below the tabs, the title 'Max Call Time' is centered. Underneath, there is a label 'Max Call Time' on the left, a text input field containing the number '5' in the center, and a note '(2~30 Min)' on the right.

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.

9.4.2. 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.

To do the configuration, you can do as follows:

1. Click **Intercom > Call Feature > Max Dial Time**
2. Click and enter the timing parameters you need.
3. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.

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

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.

9.4.3. Audio& Video Codec Configuration for SIP

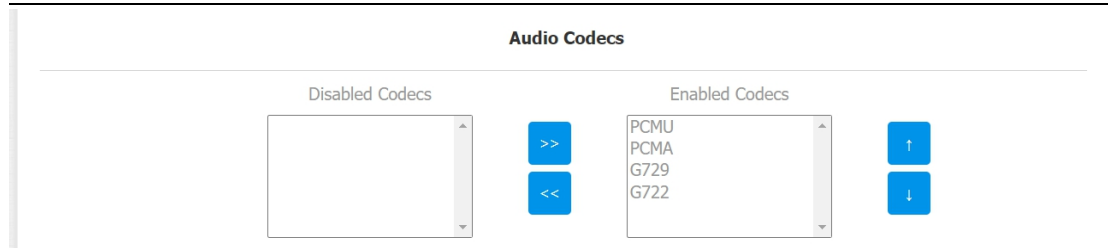
Calls

9.4.3.1. Configure Audio Codec

E16 series 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.

To do the configuration, you can do as follows:

- 1. Click **Account** > **Advanced** > **Audio Codecs***
- 2. Click on arrows and move the codec type left and right in order to enable or disable the codec function.*
- 3. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.*



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

9.4.3.2. Configure Video Codec

This series supports H.264 codec that provides a better video quality at a much lower bit rate with different video quality and payload.

To do the configuration, you can do as follows:

1. Click **Account > Advanced > Video Codec**

2. Tick the H.264 Codec name check box.
3. Set up parameters according to your need.
4. Click **Submit** tab for the validation or **Cancel** tab for the Cancellation.

Video Codecs	
Name	<input checked="" type="checkbox"/> H264
Resolution	720P ▼
Bitrate	2048 ▼
Payload	104 ▼

Parameter set-up:

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

9.5. 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.

To configure the DTMF data transmission, you can do as follows:

- 1. Click **Account > Advanced > DTMF***
- 2. Set up parameters properly according to your need.*
- 3. Press **Submit** tab for the validation or **Cancel** tab for the Cancellation.*

DTMF	
Mode	RFC2833
How to info DTMF	Disabled
Payload	101

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.

10. Relay Switch Setting

10.1. Relay Switch Setting

You can configure the relay switch(es) and DTMF for the door access on the web interface.

To do the configuration, please do as follows:

- 1. Click Access Control > Relay > Relay*
- 2. Set up relay related parameters properly according to your need.*
- 3. Click Submit tab for the validation and Cancel tab for the validation.*

Input	Relay	Web Relay	Door Log	Face Setting	CardSetting
Relay					
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"/>				
Relay Status	Relay: High				
Relay Name	<input type="text" value="Relay"/>				

Parameter Set-up:

- **Trigger Delay (Sec):** set the relay trigger delay timing (Ranging from 1-10 Sec.) For example, if you set the delay time as “5” sec. then the relay will not 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 **DMTP 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:



Note:

- If DTMF mode is set as “1 Digit DTMF” , you cannot edit

10.2. Web Relay Setting

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

10.2.1. Configure Web Relay on the Web Interface

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

To do the configuration , you can do as follows:

1. Click **Access Control > Web Relay**
2. Enter the parameters properly.
3. Go to the “**Web Relay Action Setting**” below in the same interface.
4. Configure the parameter properly.
5. Press the **Submit** tab for the validation and **Cancel** tab for the cancellation.

Input
Relay
Web Relay
Door Log
Face Setting
CardSetting
▼

Web Relay

Type

IP Address

UserName

Password

Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
Action ID 01	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 02	<input type="text"/>	<input type="text"/>	<input type="text"/>
Action ID 03	<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)

After the web relay is set up, you can configure the specific web relay to be triggered based on the relay location for the door access.

To configure the the web relay for the door access, you can do as follows:

1. Click **Access Control > User**
2. Click **Add** tab on the **User Interface** page.
3. Go to the **Access Setting** on the **Bottom**.
4. Click to select the specific web relay to be triggered at the

corresponding location in the **Web Relay** field.

5. Click **Submit** tab for the validation.

Access Setting

Web Relay





Validity Term

Submit **Back to list**

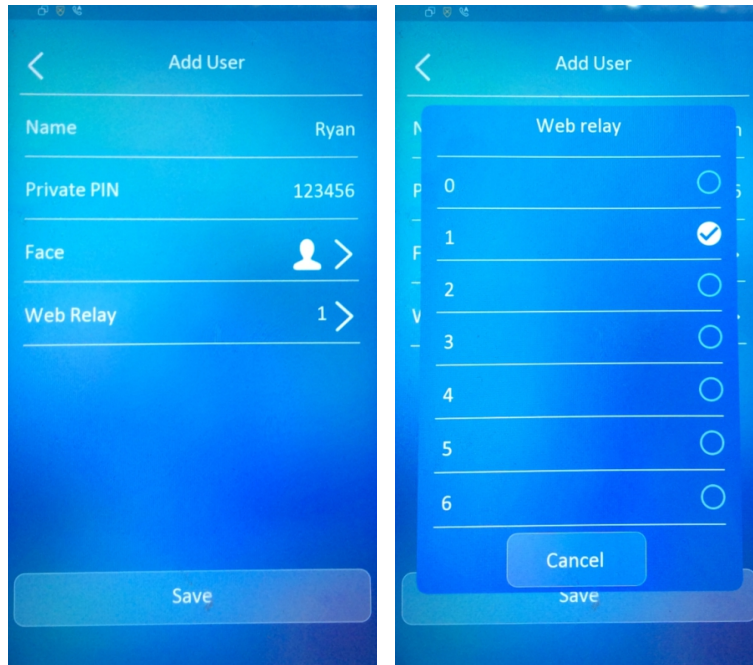
10.2.2. Configure Web Relay on the Device

You can also assign a specific web relay to a resident for the door access based on order of the the web relay set up on the web interface.

To do so , you can do as follows:

1. Press **User**  icon on the **Setting** screen.
2. Press **Add** tab.
3. Press **Web Relay**  arrow .
4. Tick the circle  icon to assign the specific web relay to a resident for the door access.

5. Press the *Save* tab on the *Add User* screen for the validation



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.

11.1.1. Create Door Access Schedule

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.

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

1. Click **Access Control > Schedule Setting**
2. Click **Schedule Type** field to select “Daily” Type.

3. Enter the schedule name.
4. Set up the daily time schedule for the validity of the door access.
5. Click **Add** tab for the validation and **Reset** tab to clear the setting.

Schedule Setting

Schedule Type: Daily

Schedule Name: [Empty Input Field]

Date Time: 00 : 00 - 00 : 00

+ Add Reset

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

1. Click **Schedule Type** field to select “Weekly” Type.
2. Enter the schedule name according to your need.
3. Select the day (s) on which door access can be valid on monthly basis.
4. Set up the time schedule for the validity of the door access during a day.
5. Click **Add** tab for the validation and **Reset** tab to clear the setting.

Schedule Type: Weekly

Schedule Name:

Day of Week: Mon Tue Wed Thur Fri Sat Sun Check All

Date Time: 00 : 00 - 00 : 00

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

1. *Click **Schedule Type** field to select “Normal” Type.*
2. *Repeat the setting in the identical way as you do for the “ Weekly” schedule.*
3. *Set the time period specifying year, month and date.*
4. *Click **Add** tab for the validation and **Reset** tab to clear the setting.*

Schedule Type: Normal

Schedule Name:

Date Range: 2020 11 25 --

Day of Week: Mon Tue Wed Thur Fri Sat Sun Check All

Date Time: 00 : 00 - 00 : 00

11.1.2. 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.

To import and export the schedule, you can do as follows:

- 1. Click Access Control > Schedule Setting> Import/Export Schedule(.xml)*
- 2. Click Select file Tab to upload your card data file.*
- 3. Click Import tab to import the file to the device.*
- 4. Click Export tab to export the file.*

Input	Relay	Web Relay	Door Log	Face Setting	CardSetting	▲
Schedule S...	Body Temp...	User	Temperatur...	BLE	PIN Setting	

Import/Export Schedule(.xml)

Not selected any files
Select File
Import
Export

 **Note:**

11.1.3. Edit the Door Access Schedule

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.

To edit or delete the schedule , you can do as follows:

1. Click **Access Control > Schedule Setting> Schedule Management**
2. Tick the schedule you wish to edit or delete .

3. Go to *Schedule Setting* section above in the same interface page.
4. Edit the schedule according to your need.
5. Click *Edit* tab for validation or *Reset* tab to go back to your previous setting

Schedule Management

<input type="checkbox"/>	Index	Type	Name	Date	Day of Week	Time
<input type="checkbox"/>	1	Daily	Daily (Work Hour) ..	-	-	09:00-18:00
<input type="checkbox"/>	2	Weekly	Weekly Cleaning	-	Mon,Wed,Fri,Sun	-
<input checked="" type="checkbox"/>	3	Normal	Day Shift	20200101-20210101	Mon,Tue,Wed,Thur,Fri,Sat,Sun	08:00-16:30

Delete
Delete All
Prev
1/1
Next
1
Page

12. Door Unlock Configuration

E16 series door phone offer you three types of door access via PIN code, RF card and Facial recognition. You can configure them on the device and web interface. 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 E16 series door phones.

12.1.1. Configur Public PIN code


You can configure and modify a total of 3 sets of separate PIN codes on the device web interface.


To configure Public PIN code, you can do as follows:

1. Click **Access Control** > **PIN Setting** > **Public PIN**
2. Tick the check box to enable the Public PIN code application.
3. Set the PIN code digit limit ranging from “4-8” in Public PIN Bits Limit field.
4. Enter the Public PIN codes.

Public PIN

Enabled	<input checked="" type="checkbox"/>
Public PIN Bits Limit	<input type="text" value="4"/>
1st Public PIN	<input type="text" value="1234"/>
2nd Public PIN	<input type="text"/>
3rd Public PIN	<input type="text"/>

 **Note:**

 **Note:**

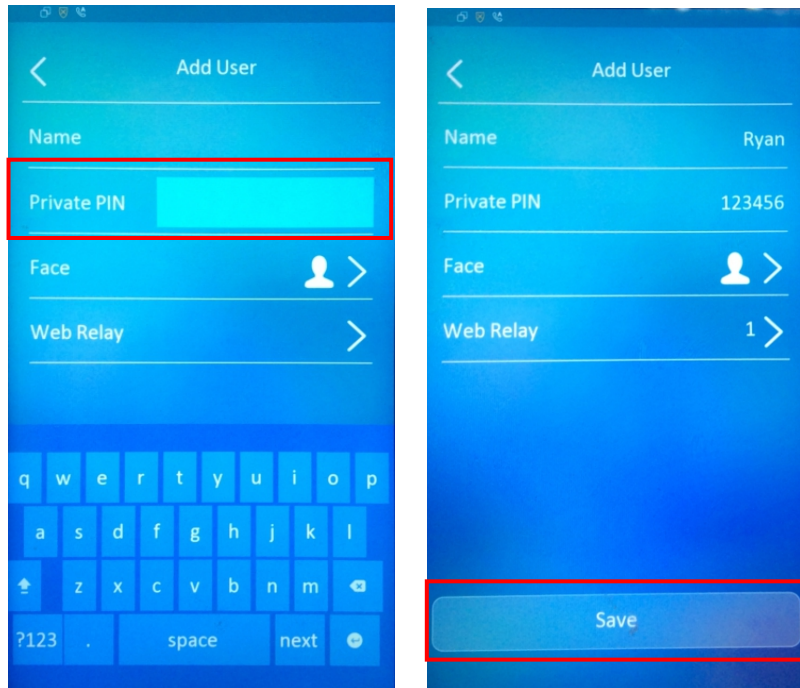
12.1.2. Configure Private PIN Code on the Device

You can configure door access by Private PIN code on the device by entering the user's name and the PIN code for the door access.

To configure private PIN code , you can do as follows:



1. Press User icon on the Setting screen.
2. Press Add tab on the bottom of the screen.
3. Enter the User name.
4. Enter the Private PIN in the Private PIN field.
5. Press Save tab on the bottom for the validation.



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.

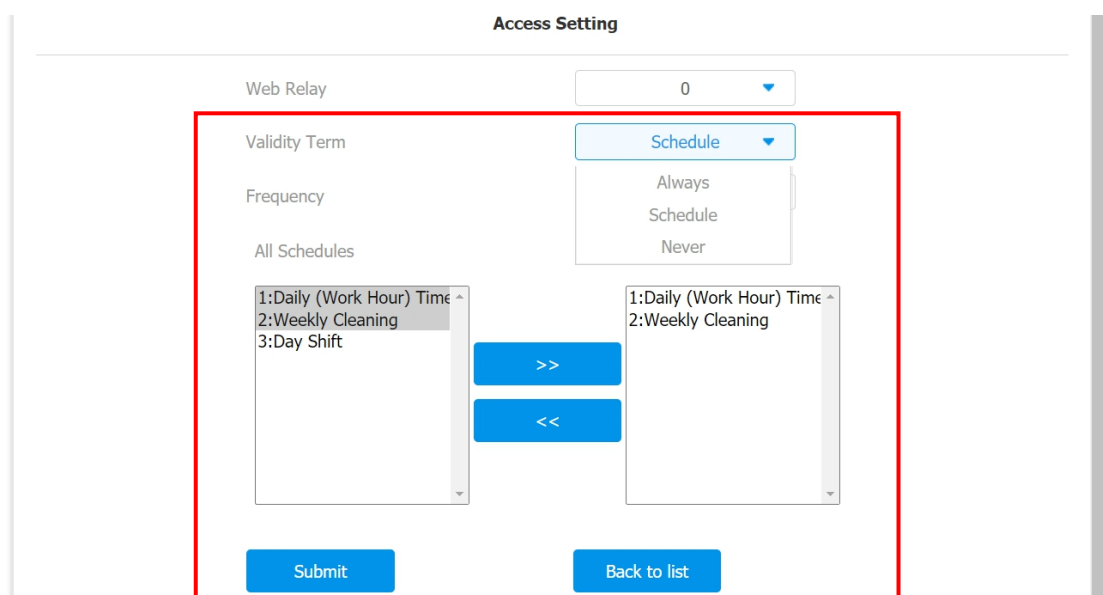
To configure PIN code , you can do as follows:

1. Click **Access Control > User**
2. Click the **Add** tab.
3. Go to **User Basic** section.
4. Enter the user's name and floor number
5. Go to **Private PIN** section.
6. Enter the private PIN code in **Code** field.
7. Click **Submit** tab for the validation.

The screenshot shows a web interface with a top navigation bar containing tabs: Input, Relay, Web Relay, Door Log, Face Setting, CardSetting, and a blue triangle icon. Below this is a sub-navigation bar with tabs: Schedule S..., Body Temp..., User (highlighted in blue), Temperatur..., BLE, and PIN Setting. The main content area is titled 'User Basic' and contains two sections. The 'User Basic' section has two input fields: 'Name' with the value 'Ryan' and 'Floor No.' with the value '403'. The 'Private PIN' section has one input field: 'Code' with the value '123456'.

To select door access Schedule for Private PIN Code door access, you can do as follows:

1. Go to **Access Setting** section in the same interface page
2. Set up PIN code validity time in the **Validity Term** field.
3. Set the limit for the total number of PIN code door access.
4. Select door access schedule for the targeted user(s).
5. Click the **Submit** tab for the validation.



Parameter Set-up:

- *Validity Term:* select validity term among three options: “Always”, “Schedule” and “Never”. if you select “Always”, then the door access via PIN code will always be valid with no restriction. If you select “Schedule”, then you are required to select among the created schedule for user-based PIN code access. If you select “Never” then the PIN code access will never be valid.
- *Frequency:* set the total number of valid PIN code access allowed.
- *All 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*

12.1.4. Configure Private PIN Access Mode

E16 series door phones offer you two types of access modes for private PIN code access, namely “PIN” and “APT#+PIN”.

To configure the access mode, you can do as follows:

- 1. Click Access Control > PIN Setting > Private PIN*
- 2. Click Authorization Mode field to select the access mode you need.*
- 3. Click Submit tab for the validation and Cancel tab for the cancellation.*

Input	Relay	Web Relay	Door Log	Face Setting	CardSetting	▲
Schedule S...	Body Temp...	User	Temperatur...	BLE	PIN Setting	
Private PIN						
Authorization Mode				<input type="text" value="PIN"/> ▼		

Parameter Set-up:

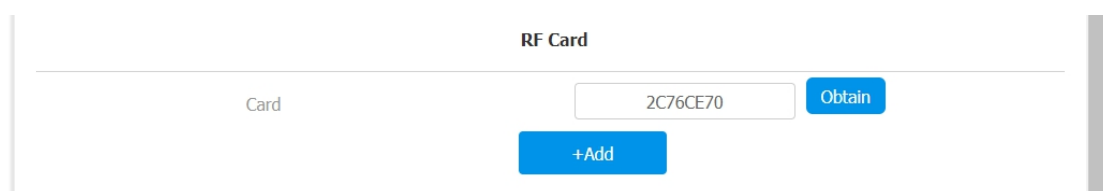
- *Authorization Mode:* select access mode between “ PIN” and “APT#+PIN”. if you select “PIN” then you are only required to enter PIN code directly for the door access, while if you select “ APT#+PIN”, then you are required to enter the Apartment Number first before entering your PIN code for the door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

12.2. Configure RF Card for Door Unlock

12.2.1. Configure RF Card on the Web Interface

To configure RF card , you can do as follows:

1. Click Access Control > User
2. Click the Add tab.
3. Go to User Basic section.
4. Enter the user's name and floor number.
5. Go to RF Card section.
6. Click and Obtain tab and place the card on the card reader area.



RF Card

Card



Note:

- Please refer to PIN code access schedule selection for the DE



Note:

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.

To select the RF card format, you can do as follows:

Input	Relay	Web Relay	Door Log	Face Setting	CardSetting ▲
Schedule S...	Body Temp...	User	Temperatur...	BLE	PIN Setting

RFID

IC-Card Display Mode

Parameter Set-up:

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

12.2.2. Configure Facial Recognition for Door Unlock

12.2.2.1. Configure Facial Recognition on the Device

To configure the facial recognition, you can do as follows:

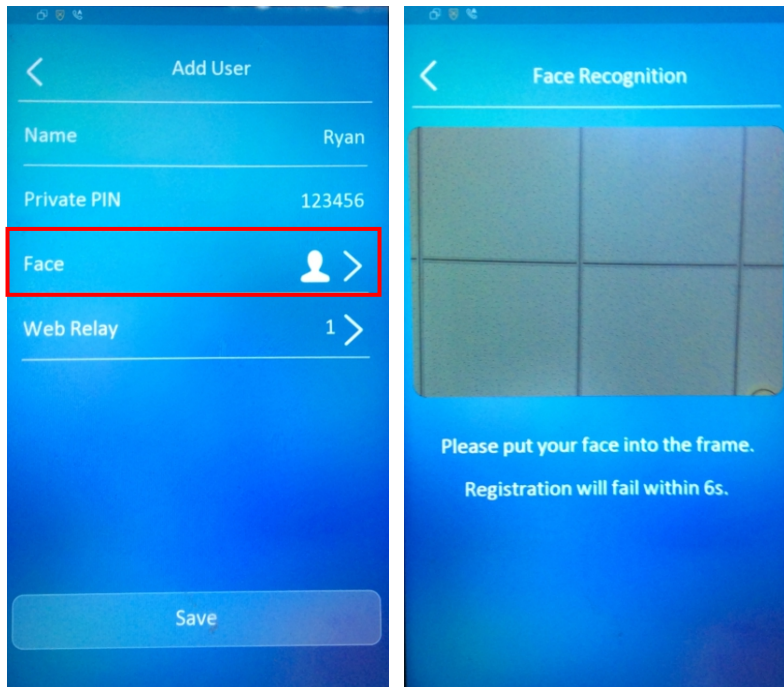
You can configure door access by facial recognition on the device by entering the user's name and register your facial ID on the device for the door access.

To configure facial recognition , you can do as follows:



1. Press **User** icon on the Setting screen.
2. Press **Add** tab on the bottom of the screen.
3. Enter the **User name**.
4. Click on **Face** for facial recognition.
5. Stand in front of door phone camera in distance between 0.5 to 1 meter and keep your face in the center of square frame for ten seconds until your facial ID is successfully collected.

6. Press *Save* tab on the bottom to save the facial registration.



12.2.2.2. Configure Facial Recognition on Web Interface

To configure PIN code , you can do as follows:

7. *Click Access Control > User*

1. *Click the Add tab.*
2. *Go to User Basic section.*
3. *Enter the user's name and floor number*
4. *Click Select File tab to upload the picture from PC for facial recognition.*
5. *Click Reset tab if you want to cancel the picture.*
6. *Click Submit tab on the bottom for the validation.*

The screenshot shows a configuration interface for facial recognition. At the top, the word "Face" is centered. Below it, there is a horizontal line. Under the line, the word "Status" is on the left and "UnRegistered" is on the right. Below "Status", the text "Photo(jpg/png)" is displayed. To the right of this text is a file selection area containing the text "Not selected any files", a blue "Select File" button, and a grey "Reset" button.

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:

12.3. Configure Door Access Using Configured Files.

E16 series door phones allow you to speedily configure user(s)-specific door access in batch by importing the configured all-in-one door access control files incorporating user information, door access type,

door access schedule etc., thus all the door access 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.

To import the configured door access files, you can do as follows:

1. Click **Access Control > User**
2. Click **Select File** tab in **User Data (except Face)** field to upload the configured file for the door access not inclusive of the access by facial recognition.
3. Click **Import** tab to start uploading the files and **Export** to export the file.
4. Click **Select File** tab in **Face** field to upload configured file for the door access by facial recognition.
5. Click **Import** tab to start uploading the files and **Export** to export the file.
6. Click **Reset** tab if your want to clear the configured file (facial recognition) you selected.

Import/Export User

User Data(Except Face)	Not selected any files	Select File	Import	Export	
Face	Not selected any files	Select File	Import	Export	Reset

**Note:**

- *Configured file for facial recognition and the other types of*

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




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

To search and edit the user data, you can do as follows:

1. Click Access Control > User

2. Enter the search information in the **Search** field and press **Reset** tab if you want to clear the information entered.
3. Click **Edit** tab to add the user data.
4. Tick the check box of the specific user if you want to delete the user or tick the check box by the **Index** to delete all the user data.

User

<input type="checkbox"/>	Index	Name	PIN	RF Card	Frequency	Floor No.	Relay	Edit
<input checked="" type="checkbox"/>	1	Ryan			0	403	1	
<input type="checkbox"/>								
<input type="checkbox"/>								

12.4.1. Unlock by QR Code

QR code is another option for door access. If you want to apply QR code access, you need to enable the QR code function.

To enable the QR code function , you can do as follows:

1. Click *Access Control > Relay > Open Relay via QR Code*
2. Enable the QR code function by clicking "On" in the *Enable* field.
3. Click *Submit* tab for validation and *Cancel* tab for cancellation.

Open Relay Via QR Code

Enable



Note:

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.

1. Click *Access Control > BLE > BLE*

2. Set up parameter according to your need.
3. Click on **Submit** tab for the validation and **Cancel** tab for the cancellation.

The screenshot shows a web interface for configuring BLE settings. At the top, there are several tabs: Input, Relay, Web Relay, Door Log, Face Setting, CardSetting, Schedule S..., Body Temp..., User, Temperatur..., BLE (selected), and PIN Setting. Below the tabs, the BLE configuration section is visible. It includes an 'Enabled' checkbox which is checked. Below that is an 'Rssi Threshold' input field containing the value '72', with a range of '(-85~-50DB)' indicated to the right. Underneath is an 'Open Door Interval' dropdown menu showing '5' and '(Sec)' to its right. At the bottom of the configuration area, there are two blue buttons: 'Submit' and 'Cancel'.

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 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.

To do the configuration, you can do as follows:

- 1. Click Access Control > Relay > Open Relay via HTTP*
- 2. Set up parameters properly.*
- 3. Click Submit tab for the validation and Cancel tab for the cancellation.*

Open Relay via HTTP

Enable	<input type="button" value="OFF"/>
User Name	<input type="text"/>
Password	<input type="password" value="....."/>

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/cgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1>



Note:

• DoorName in the HTTP command above refers to the relay

12.4.4. 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 door phone Input to trigger the relay for the door access.

To do the configuration, you can do as follows:

1. Click **Access Control > Input > Input**
2. Tick **Enabled** to enable the Input function.
3. Set up the parameters according to your need.
4. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.

Input
Relay
Web Relay
Door Log
Face Setting
CardSetting
▼

Input

Enabled	<input checked="" type="checkbox"/>
Trigger Electrical Level	<div style="border: 1px solid #ccc; padding: 2px 5px; display: inline-block;">Low ▼</div>
Execute Relay	<div style="border: 1px solid #ccc; padding: 2px 5px; display: inline-block;">Relay ▼</div>
Door Status	Door: High

Submit

Cancel

Parameter set-up:

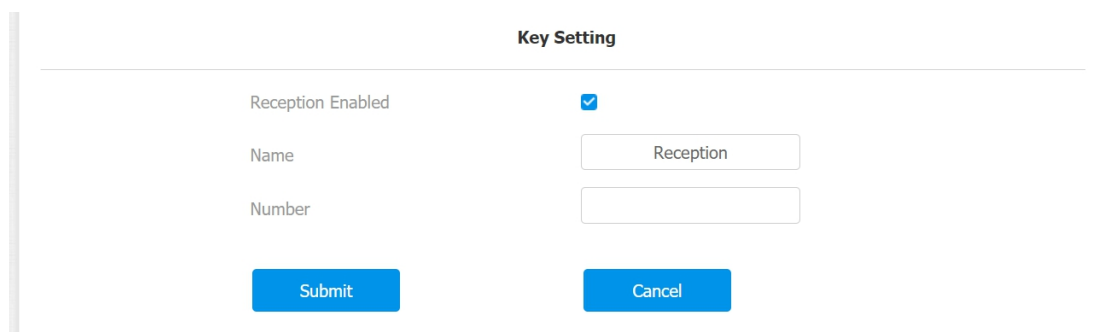
- *Trigger Electrical Level: select the trigger electrical level options between “High” and “Low” according the actual operation on the e x i t b u t t o n .*
- *Execute Relay: set up relays to be triggered by the input.*
- *Door Status: display the status of input signal.*

12.4.5. Unlock by Reception Tab

In the device home screen, E16 series door phone provide residents and visitors a quick door access by pressing the **Reception** tab on the bottom of the home screen.

To do the configuration, you can do as follows:

1. Click **Intercom > Basic > Key Setting**
2. Set the parameters properly.
3. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.

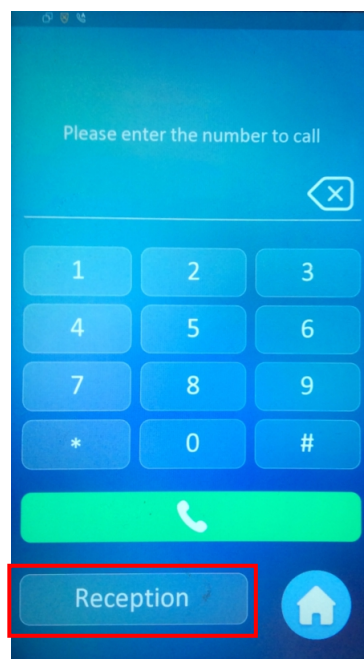


Key Setting

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.



12.4.6. Unlock by DTMF Code

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.

To do the extra DTMF configuration on the web interface, you can do as follows:

- 1. Click Account > Advanced > DTMF*
- 2. Set up parameters properly.*
- 3. Click Submit tab for the validation and Cancel tab for the cancellation.*

Parameter Set-up:

DTMF

Type	<input type="text" value="RFC2833"/>	How To Notify DTMF	<input type="text" value="Disabled"/>
DTMF Payload	<input type="text" value="101"/>	(96~127)	

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



Note:

- *Please refer to the chapter **Configure DTMF Data***

12.4.7. Body Temperature Measurement for Door Access (Optional)

E16 series 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.

To do the configuration, you can do as follows:

1. Click *Access Control > Body Temperature > Measuring Body Temperature*
2. Set up parameters properly.
3. Set the schedule for the validity of the body temperature measurement.
4. Click on *Submit* tab for the validation and *Cancel* tab for the cancellation.

The screenshot shows the 'Measuring Body Temperature' configuration page. At the top, there are navigation tabs: Input, Relay, Web Relay, Door Log, Face Setting, CardSetting, and a dropdown arrow. Below these are sub-tabs: Schedule S..., Body Temp... (selected), User, and Temperatur... The main content area is titled 'Measuring Body Temperature' and contains the following settings:

- Mode:** Disabled (dropdown menu)
- Mask Detection:** Disabled (dropdown menu)
- Temperature Unit:** Centigrade (dropdown menu)
- Normal Body Temperature:** 37.3 (text input) (Below 37.3 °C)
- (If the detected temperature is lower than 34 °C, the device will prompt low temperature, please try again later)**
- Action To Execute:** SIP/ IP Call
- SIP/ IP Call Number:** (empty text input)

Parameter set-up:

- **Mode:** select either “Disabled” Mode or “Wrist” Mode for temperature measurement according to your need. The device can

be installed with digital forehead temperature detector therefore you can be required to set the mode properly according to your application.

- **Mask Detection:** select “Enable” or “Disable” to turn on or turn off the mask detection. When enabled, the device will check if the visitor is wearing a mask or not while reminding the visitor with the announcement “Please wear a mask” while visitors wearing mask will be prompted either “Keep face in the frame” or “Keep wrist close to the sensor” depending on the mode that is selected. 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.

- *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.

12.4.7.2. Ambient Temperature Configuration

In order to offset the minor variations on the temperature as affected by the ambient temperature in the different places where the device is installed or in the different time of a day, you are required to configure the temperature setting on the basis of time segments during a day.

To do the configuration, you can do as follows:

1. Click *Access Control > Body Temperature > Ambient Temperature Setting*
2. Set up parameters properly.
3. Click *Submit* tab for the validation or *Cancel* tab for the cancellation.

Ambient Temperature Setting

ID	Start Time	End Time	Ambient Temperature
1	02 ▾ : 00 ▾	08 ▾ : 00 ▾	25.0 (10~40.0°C)
2	08 ▾ : 00 ▾	14 ▾ : 00 ▾	25.0 (10~40.0°C)
3	14 ▾ : 00 ▾	20 ▾ : 00 ▾	25.0 (10~40.0°C)
4	20 ▾ : 00 ▾	02 ▾ : 00 ▾	25.0 (10~40.0°C)

Submit
Cancel

Parameter Set-up:

- *Start Time/End Time:* select the start time and end time temperature by referring to the actual temperature measured at the time segments ranging from 10- 40°Cdegree Celsius. For example, when you divide the time into four time segments, then

each of the time segments will be six hours (24 hours a day), while the end time of one segment should be the start time of the next time segment. You can divide the time segments according to your need.

- **Ambient Temperature:** enter the ambient temperature degree. Accuracy can be ensured for the actual temperature value within the range from 10- 40 degree Celsius .

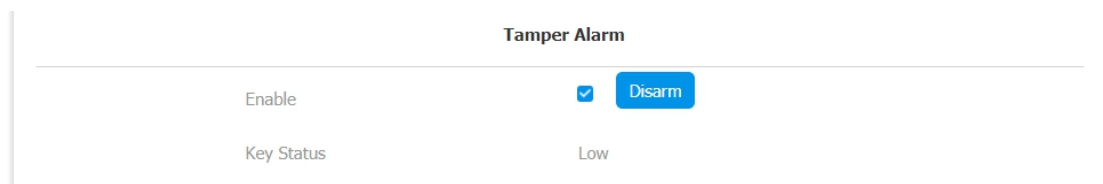
13. Security

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.

To set up the temper alarm , you can do as follows:

1. Click *Security > Basic > Temper Alarm*
2. Tick the check box to enable the temper alarm function.



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 be appeared, the temper alarm is cleared



Note:

The

13.2. Motion Detection

13.3. Security Notification Setting

13.3.1. Email Notification Setting

If you want to receive the security notification via email, you can configure the Email notification on the web interface properly.

To do the configuration, you can do as follows:

1. Click **Setting > Action > Email Notification**

2. Set up parameters properly according to your need.
3. Click **Submit** tab for validation and **Cancel** tab for cancellation.

Time/Lang	Action	Door
Email Notification		
Sender's Email Address	<input type="text"/>	
Sender's Email Name	<input type="text"/>	
Receiver's Email Address	<input type="text"/>	
Receiver's 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"/>	

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.*

13.3.2. FTP Notification setting

If you want to receive the security notification via FTP, you can configure the FTP notification on the web interface properly.

To do the configuration, you can do as follows:

1. Click **Setting > Action > FTP Notification**
2. Set up parameters properly according to your need.
3. Click **Submit** tab for validation and **Cancel** tab for cancellation.

FTP Notification	
FTP Server	<input type="text"/>
FTP User Name	<input type="text"/>
FTP Password	<input type="password" value="....."/>
FTP Path	<input type="text"/>

Parameter set-up:

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

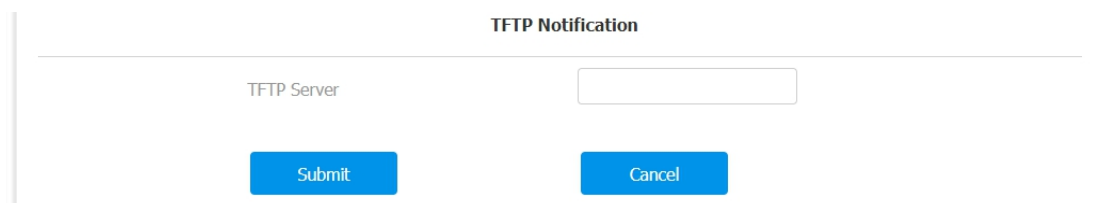
- **FTP User Name:** enter the FTP server user name.
- **FTP Password:** enter the FTP server password.
- **FTP Path:** enter the folder name you created in FTP server.

13.3.3. TFTP Notification Setting

If you want to receive the security notification via TFTP, you can configure the FTP notification on the web interface properly.

To do the configuration, you can do as follows:

1. Click **Setting > Action > TFTP Notification**
2. Set up parameters properly according to your need.
3. Click **Submit** tab for validation and **Cancel** tab for cancellation.



The screenshot shows a web interface titled "TFTP Notification". Below the title is a horizontal line. Underneath the line, the text "TFTP Server" is followed by an empty text input field. Below the input field are two blue buttons: "Submit" on the left and "Cancel" on the right.

Parameter set-up:

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

13.4. 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.

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

- 1. Click Security > Basic > Session Time Out*
- 2. Enter the time-out value in the Session Time Out Value field.*
- 3. Click Submit tab for the validation and Cancel tab for the cancellation.*

Session Time Out

Session Time Out Value

14. Monitor and Image

14.1. Mjpeg Image Capturing

E16 series 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.

To do the configuration, you can do as follows:

1. Click *Surveillance > MJPEG > Mjpeg Server*
2. Set the parameters properly according to your need.
3. Click *Submit* tab for the validation and *Cancel* tab for the

cancellation.

RTSP MJPEG Onvif Live Stream

MJPEG Server

Enabled

Image Quality 1080P

Submit Cancel

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:

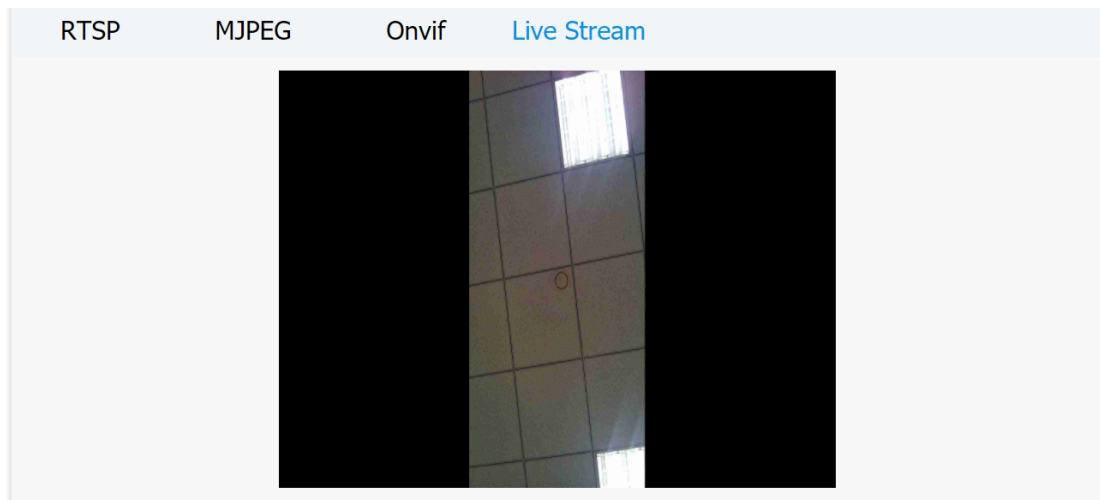
1. Enter “http://192.168.1.104:8080/picture.jpg” on the web browser
2. Ppress Enter key in your keyboard to capture the image.

14.2. Live Stream

If you want to check the real-time video from the E16 series door phone, 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.

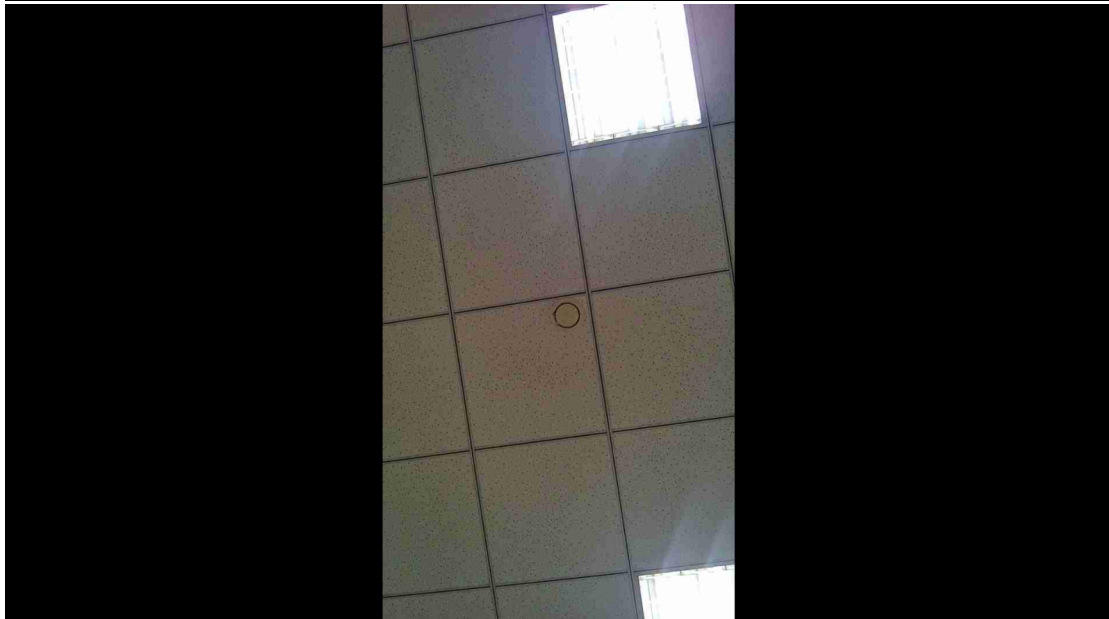
To check the real time video on the web interface, you can do as follows:

1. Click *Surveillance > Live Stream*
2. Check the real time video on the web interface.



To check the real time video using URL, you can do as follows:

1. Enter the correct URL (http://IP_address:8080/video.cgi) on the web browser if you want to obtain the real-time video directly with going to the web interface.
2. Check the real time video.



14.3. RTSP Stream Monitoring

E16 series door phone support 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.

To do the configuration, you can do as follows:

1. Click **Surveillance > RTSP > RTSP Basic**
2. Set up parameters properly.
3. Click **Submit** tab for validation and **Cancel** tab for cancellation.

RTSP	MJPEG	Onvif	Live Stream
RTSP Basic			
Enabled	<input checked="" type="checkbox"/>		
Authorization Enabled	<input type="checkbox"/>		
Authorization Mode	<input type="text" value="Digest"/>		
User Name	<input type="text" value="admin"/>		
Password	<input type="password" value="....."/>		

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.

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. which based on your actual network environment on the web

interface.

To configure the parameters, please do as follows:

1. Click *Surveillance > RTSP > H.264 Video Parameters*
2. Set up video parameters according to your need.
3. Click *Submit* tab for validation and *Cancel* tab for cancellation.

H.264 Video Parameters

Video Resolution	<input type="text" value="1080P"/>
Video Framerate	<input type="text" value="25 fps"/>
Video Bitrate	<input type="text" value="4096 kbps"/>
2nd Video Resolution	<input type="text" value="VGA"/>
2nd Video Framerate	<input type="text" value="25 fps"/>
2nd Video Bitrate	<input type="text" value="512 kbps"/>

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 kpbs” according to your network environment. The default video bit-rate is “ 2048 kpbs”.
- **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 kpbs” by default.



Note:

14.4. ONVIF

Real-time video from the E16 series door phone 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.

To do the configuration, you can do as follows:

1. Click *Intercom > ONVIF*
2. Set up parameters properly.
3. Click *Submit* tab for validation and *Cancel* tab for cancellation.

RTSP MJPEG **Onvif** Live Stream

Basic Setting

Discoverable

User Name

Password

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:

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.

To check the call log, you can do as follows:

- 1. Click Intercom > Call Log*

2. Click *Call history* field to select specific type of call log.
3. Click *Export* tab if you want to export the call log.
4. Check the specific call log check box and click *Delete* tab to delete.
5. Click *Delete all* tab if you want to delete all of the call logs.

The screenshot shows the 'Call Log' section of the interface. It includes a 'Call History' dropdown menu set to 'All' and an 'Export' button. Below is a table with the following data:

Index	Type	Date	Time	Local Identity	Name	Number
<input checked="" type="checkbox"/>	1	Dialed	2020-11-24	06:47:07	14@192.168.3 5.114	Indoor Monitor 192.168.35.1 26@192.168.3 5.126
<input type="checkbox"/>	2	Dialed	2020-11-24	06:46:46	14@192.168.3 5.114	Indoor Monitor 192.168.35.1 26@192.168.3 5.126
<input type="checkbox"/>	3	Dialed	2020-11-24	06:46:13	14@192.168.3	Indoor Monitor 192.168.35.1 26@192.168.3

At the bottom, there are buttons for 'Delete', 'Delete All', 'Prev', 'Next', and 'Page'.

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.

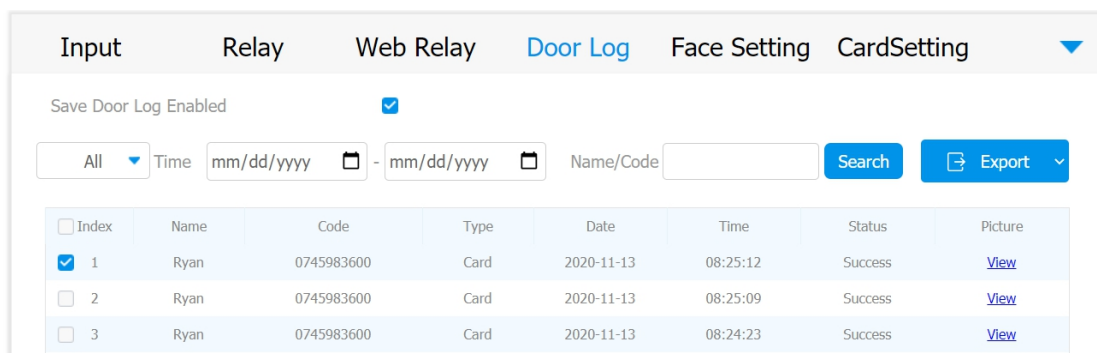
15.2. Door Logs

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

and check the door logs on the device web interface.

To access the door logs , you can do as follows:

1. Click **Access > Door log**
2. Tick the the check box of **Save Door Log Enabled** if you want to save the log.
3. Click  icon if you want to search door access by “ All” “ Success” and “failed “.
4. Click on “**View**” on each door log if you want to see the picture captured for the door log.
5. Check on the specific door log check box and click **Delete** tab to delete.
6. Click **Delete all** tab if you want to delete all of the door logs.



The screenshot shows the 'Door Log' tab in the Akuvox Admin Interface. At the top, there are navigation tabs: Input, Relay, Web Relay, Door Log (selected), Face Setting, and CardSetting. Below the tabs, there is a 'Save Door Log Enabled' checkbox which is checked. There are also date pickers for 'Time' and 'Name/Code', a 'Search' button, and an 'Export' button. Below this is a table with the following data:

<input type="checkbox"/> Index	Name	Code	Type	Date	Time	Status	Picture
<input checked="" type="checkbox"/> 1	Ryan	0745983600	Card	2020-11-13	08:25:12	Success	View
<input type="checkbox"/> 2	Ryan	0745983600	Card	2020-11-13	08:25:09	Success	View
<input type="checkbox"/> 3	Ryan	0745983600	Card	2020-11-13	08:24:23	Success	View

Selected:1/1

Delete Delete All 

Total:1

Prev

1/1

Next

Go To Page

1

Page

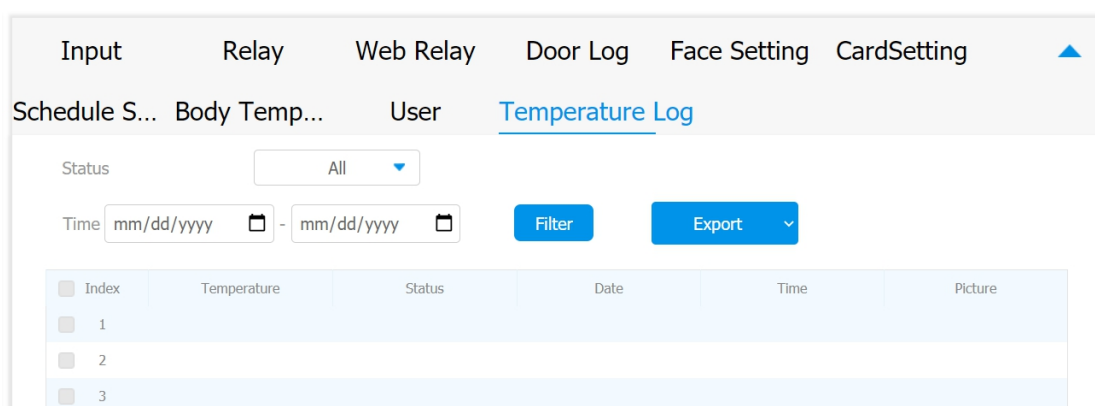
Parameter set-up:

- *Save Door Log Enabled:* Tick the check box to turn on or turn off the door log function.
- *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.

15.3. Temperature Log

To check temperature log, you can do as follows:

1. Click **Access Control > Temperature Log**
2. Click **Status** field to select the range and category of temperature log check among four options: “All”, “Normal”, “Abnormal”, “Low Temperature”.
3. Click **Filter** tab to see the specific category of temperature log selected.
4. Click **Export** tab to export the the temperature log.
5. Click the specific check box and click **Delete** tab to delete the temperature log you want to delete.
6. Tick the the check box by **Index** to delete all the temperature log.



16. Debug

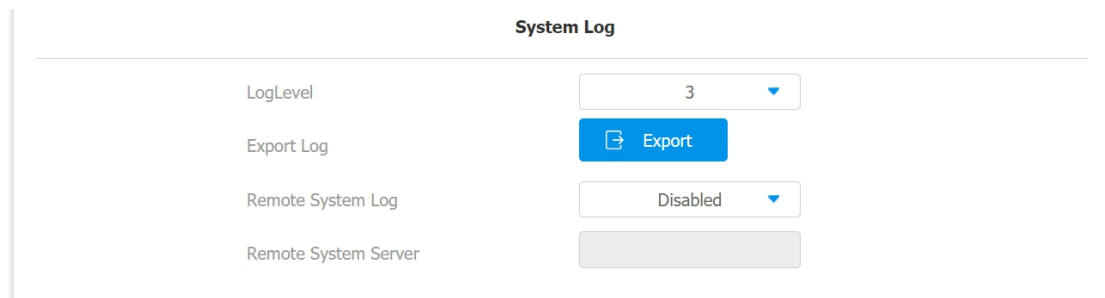
16.1. System Log for Debugging

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.

To do the configuration, you can do as follows:

- 1. Click Upgrade > Advanced > System Log*
- 2. Enter the parameters properly.*
- 3. Reproduce the problem occurred.*

4. Click **Export** tab to export logs.
5. Click **Submit** tab for validation and **Cancel** for cancellation.



The screenshot shows a configuration panel titled "System Log". It contains four rows of settings:

Parameter	Value
LogLevel	3
Export Log	Export
Remote System Log	Disabled
Remote System Server	

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:** select “Enable” or “Disable” if you want to

enable or disable the remote system log.

- *Remote System Server: enter the remote server address to receive the the device log. And the remote server address will be provide by Akuvox technical support.*

16.2. PCAP for Debugging

PCAP in E16 series door phone 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.

To do the configuration, you can do as follows:

- 1. Click Upgrade > Advanced > PCAP*
- 2. Set up parameters properly.*
- 3. Start PCAP data packets capturing by clicking on Start tab.*
- 4. Stop PCAP data packets capturing by clicking on the Stop tab.*
- 5. Export the data packets captured by PCAP by clicking on Export*

tab.

PCAP

Specific Port	<input type="text" value="1~65535"/>		
PCAP	<input type="button" value="Start"/>	<input type="button" value="Stop"/>	<input type="button" value="Export"/>
PCAP Auto Refresh	<input style="width: 100%;" type="text" value="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 50M 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.

17. Firmware Upgrade

Firmwares of different versions for E16 series door phone can be upgraded on the device web interface.

To upgrade the firmware, you can do as follows:

1. Click *Upgrade > Basic*
2. Select firmware files from your local PC.
3. Press *Submit* tab for the validation and *Cancel* tab for the cancellation.

The screenshot shows the 'Basic' settings page. At the top, there are two tabs: 'Basic' (selected) and 'Advanced'. Below the tabs, there are several rows of settings:

Firmware Version	116.30.0.28
Hardware Version	116.0.5.1.0.0.0.0
Upgrade	Not selected any files <input type="button" value="Select File"/> <input type="button" value="Submit"/> <input type="button" value="Cancel"/>
Reset To Factory Setting	<input type="button" value="Submit"/>
Reboot	<input type="button" value="Submit"/>

The 'Upgrade' row is highlighted with a red border. The 'Submit' and 'Cancel' buttons in this row are blue.



Note:

18. Backup

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

To do so , you can do as follows:

1. Click **Upgrade > Advanced > Others**
2. Click **Select File** to select the file from your local PC.
3. Click **Import** tab if you want to import the selected config file.
4. Click **Export** tab if you want to export the existing config files to you local PC.
5. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.

The screenshot shows a web interface titled "Others". At the top, it says "Config File(.tgz/.conf/.cfg)". Below this is a file selection area with the text "Not selected any files" and a blue "Select File" button. Underneath are two blue buttons: "Import" with a folder icon and "Export" with a folder icon and the text "(Encrypted)". At the bottom, there are two more blue buttons: "Submit" and "Cancel".

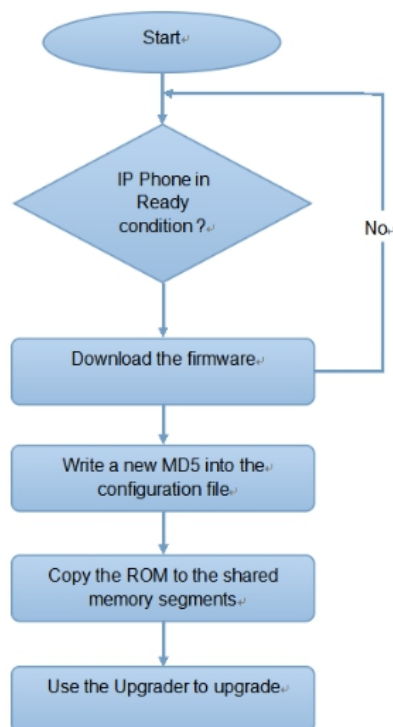
19. Auto-provisioning via Configuration File

Configurations and upgrading on E16 series door phone can be done on the web interface via one-time auto-provisioning and scheduled auto-provisioning via configuration files, thus saving you from setting up configuration needed one by one manually on the door phone.

19.1. Provisioning Principle

Auto-provisioning is a feature used to configure or upgrade the devices

in batch via third party servers. DHCP, PNP, TFTP, FTP, HTTPS are the protocols used by the Akuvox intercom devices to access the URL of the address of the third party server which stores configuration files and firmwares, which will then be used to to update the firmware and the corresponding parameters on the door phone.



19.2. 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: r000000000083.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*

19.3. 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.

To set up the schedule, you can do as follows:

1. Click *Upgrade > Advanced > Automatic Autop*
2. Set up mode and schedule according to your need.
3. Click *Submit* tab for the validation and *Cancel* tab for the cancellation.

Automatic Autop

Mode: Power On

Schedule: Sunday

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

Clear MD5

Export Autop Template

Submit

Export

Parameter Set-up:

- **Power On:** select “Power on”, if you want the device to perform Autop every time it boots up.
- **Repeatedly:** select “ Repeatedly”, if you want the device to perform autop according to the schedule you set up.

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

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.

To set up DHCP AutoP with “Custom Option” and “Power on” mode, you can do as follows:

1. Click Upgrade > Advanced > Automatic Autop
2. Click Export tab in Export Autop Template to export Autop template.
3. Set up DHCP Option on DHCP server.

Automatic Autop

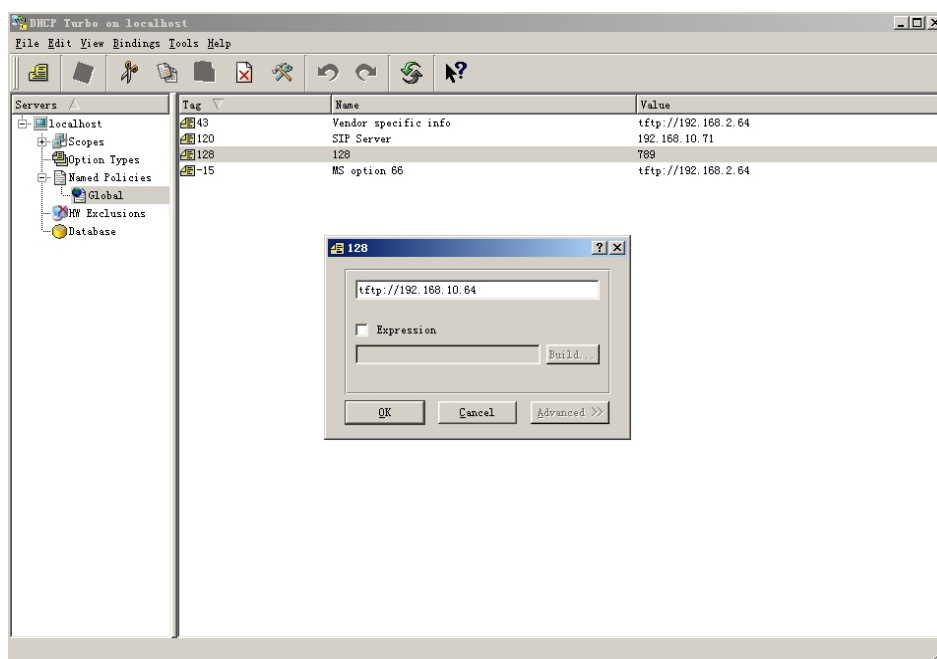
Mode: Power On ▼

Schedule: Sunday ▼

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

Clear MD5 Submit

Export Autop Template Export





Note:

- The custom Option type must be a string. The value is the URL.

4. Rename the AutoP config template.
5. Select general provisioning configuration file for the device in-batch provisioning or the MAC-based configuration file for the specific device provisioning.
6. Upload firmware to DHCP/TFTP/FTP/HTTP/HTTPS server.
7. Edit AutoP config template.
8. Go to **Upgrade > Advanced > DHCP Option** on the device web interface.
9. Enter the DHCP code in the **Custom Option** field for the URL to the config file server.
10. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.

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 E16 as an example “r000000000016.cfg” (10 “zeros” in total while the

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.

To set up static provisioning autop, you can do as follows

1. Click Upgrade > Advanced > Automatic Autop

2. Click *Export* tab in *Export Autop Template* to export Autop template.

The screenshot shows the 'Automatic Autop' configuration interface. It includes a 'Mode' dropdown set to 'Power On', a 'Schedule' dropdown set to 'Sunday', and two input fields for 'Hour(0~23)' (22) and 'Min(0~59)' (0). Below these are 'Clear MD5' and 'Submit' buttons. At the bottom, there is an 'Export Autop Template' label and an 'Export' button with a download icon, which is highlighted by a red rectangular box.

3. Rename the AutoP config template.
4. Select general provisioning configuration file for the device in-batch provisioning or the MAC-based configuration file for the specific device provisioning. (for example: `r0000000000016` for E16 door phone and `r0000000000115` for C315 in door monitor)
5. Upload firmware to DHCP/TFTP/FTP/HTTP/HTTPS server.
6. Edit AutoP config template.
7. Upload the AutoP config template to DHCP/TFTP/FTP/HTTP/HTTPS server.
8. Go to **Upgrade > Advanced > Manual Autop** on the web interface.
9. Enter TFTP URL into the box(under the path "Upgrade-Advanced") and click AutoP Immediately.

Manual Autop	
URL	<input type="text" value="tftp://192.168.35.98"/>
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>
Common AES Key	<input type="password" value="....."/>
AES Key(MAC)	<input type="password" value="....."/>
AutoP Immediately	<input type="button" value="AutoP Immediately"/>

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:



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)



Tip:

- *Akuvox do not provide user specified server.*

20. Integration with Third Party Device

20.1. Integration via Wiegand

If you want to integrate the E16 series door phone with the third party devices via Wiegand, you can configure the Wiegand on the web interface.

1. Click **Device > Wiegand > Wiegand**
2. Set up parameters according to your need.
3. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.

Light	Wiegand	RS485	Voice	LCD
Wiegand				
Wiegand Display Mode		8HN ▼		
Wiegand Card Reader Mode		Wiegand-26 ▼		
Wiegand Transfer Mode		Input ▼		
Wiegand Input Data Order		Normal ▼		
Wiegand Output Data Order		Normal ▼		
Wiegand Output CRC		<input checked="" type="checkbox"/>		
Submit		Cancel		

Parameter set-up:

- **Wiegand Display Mode:** select Wiegand 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 Transfer Mode:* set the Transfer mode between “Input” or “ Output” if the door phone is used as a receiver then set it as “ Input” for the door phone and vice versa.
- *Wiegand Input Data Order:* set the Wiegand input data sequence between “ Normal” and “Reversed” if you select “ Reversed” then the input card number will be reversed 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 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.

To do the configuration, you can do as follows:

1. Click **Device > RS485 > RS485 List**
2. Set up parameter properly.
3. Click **Submit** tab for the validation or **Cancel** tab for the cancellation.

Light	Wiegand	RS485	Voice	LCD
RS485 List				
Apply to		OSDP ▼		

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.*

<i>NO.</i>	<i>Integration Mode</i>	<i>Description</i>
<i>1</i>	<i>None</i>	<i>If you select "None" then the RS485 integration will be disabled.</i>
<i>2</i>	<i>OSDP</i>	<i>If you Select "OSDP" Mode, then the integration communication between the</i>

20.3. OSDP Setting

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.

To do the configuration, please do as follows:

1. Click **Device** > **RS485** > **OSDP Advance Setting**
2. Set up parameter properly.
3. click **Send** tab if you want to send the Dummy Card number to be authenticated by the third party device.
4. Click **Submit** tab for the validation and **Cancel** tab for the cancellation.

OSDP Advance Setting

Connect Status: Disconnected

Output With: Wiegand

Submit Cancel

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:

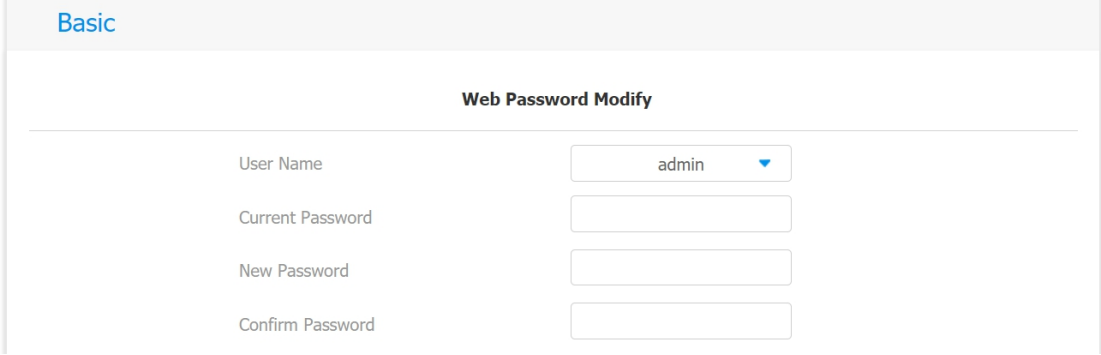
21. Password Modification

On the device web interface, you can set and change both the project

PIN Code for accessing the device setting and password for accessing the web interface. In addition, you can also select the user role when setting passwords.

To set and change the web interface passwords, you can do as follows:

- 1. Click Security > Basic > Web Password Modify*
- 2. Select User Name between "admin".*

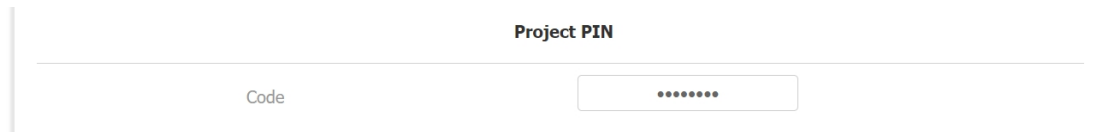


The screenshot shows a web interface with a header labeled 'Basic'. Below the header is a section titled 'Web Password Modify'. This section contains four input fields arranged in two columns. The first row has 'User Name' on the left and a dropdown menu on the right showing 'admin'. The second row has 'Current Password' on the left and an empty text input field on the right. The third row has 'New Password' on the left and an empty text input field on the right. The fourth row has 'Confirm Password' on the left and an empty text input field on the right.

To set up the Project PIN code, you can do as follows:

- 1. Go to Project PIN section in the same interface page.*
- 2. Set up or modify the device setting PIN code.*

3. Click *Submit* tab for the validation and *Cancel* tab for the cancellation.



A screenshot of a web form titled "Project PIN". It features a single input field with a placeholder text "Code" and a masked password field containing seven dots. The form is enclosed in a light gray border.

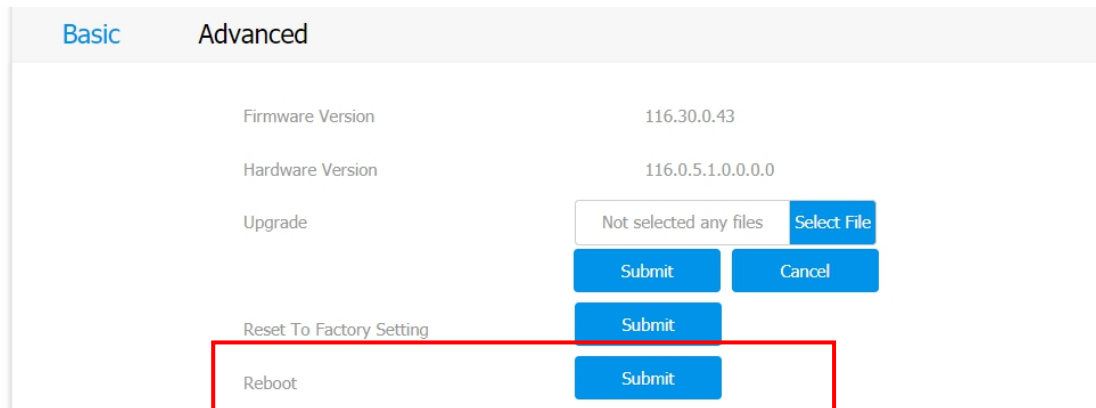
22. System Reboot&Reset

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.

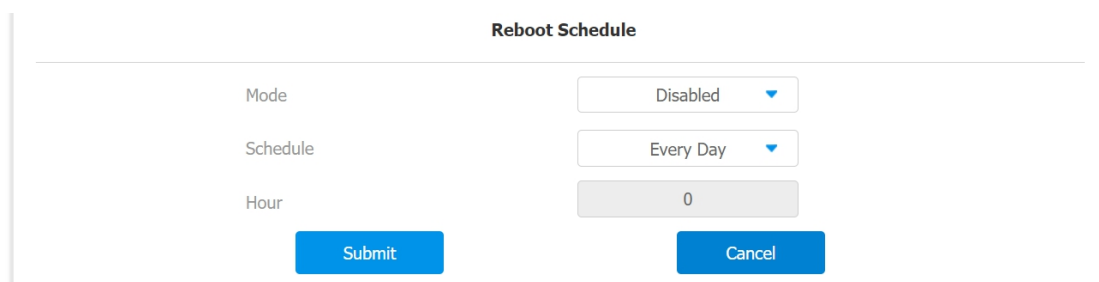
To restart the system setting on the web interface, you can do as follows:

1. Click Upgrade > Basic
2. Click on Submit tab for restarting the device.



To set up the device restart schedule, you can do as follows:

1. Click Upgrade > Advanced > Reboot Schedule
2. Enable the scheduled Reboot mode.
3. Set up the device restart day and timing (0-23).
4. Click Submit tab for the validation and Cancel tab for the cancellation.



22.2. Reset

If you want to reset the device system to the factory setting, you can it on the web interface.

To reset to the factory setting, you can do as follows:

1. Click Upgrade > Basic
2. Click on Submit tab for Reset to Factory Setting.

The screenshot shows a web interface with two tabs: 'Basic' (selected) and 'Advanced'. Under the 'Basic' tab, there are several rows of information and actions:

Firmware Version	116.30.0.43
Hardware Version	116.0.5.1.0.0.0.0
Upgrade	Not selected any files <input type="button" value="Select File"/>
	<input type="button" value="Submit"/> <input type="button" value="Cancel"/>
Reset To Factory Setting	<input type="button" value="Submit"/>
Reboot	<input type="button" value="Submit"/>

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

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

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 status 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;

3. 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

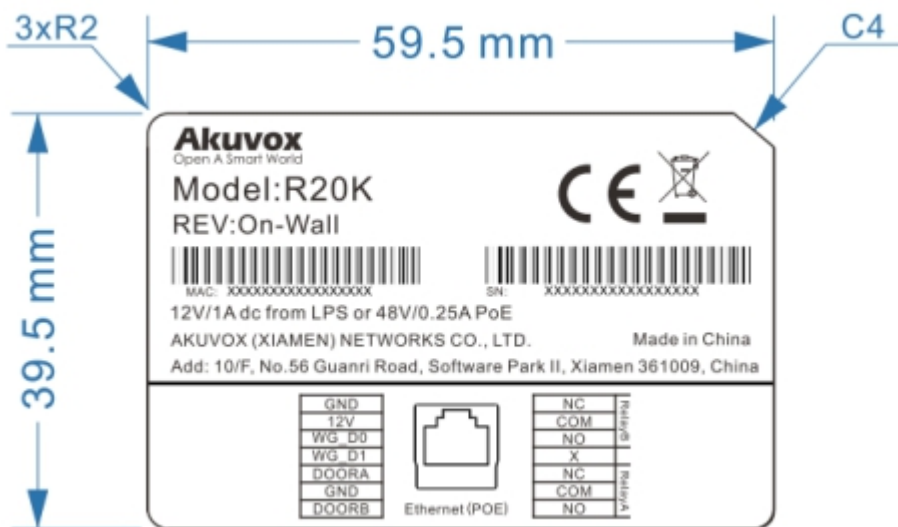
Q6: Do door phones support these card types? Prox, Legacy iClass,iClassSE,HID Mifare, HID DESFire,HID SEOS

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.

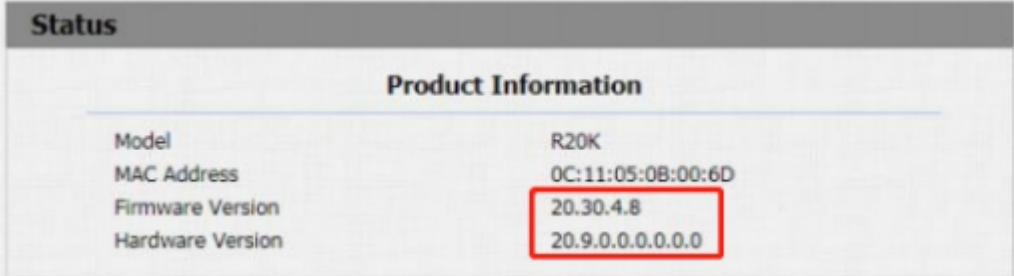
220.X.X.X is hardware version 2.

- **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.



Status	
Product Information	
Model	R20K
MAC Address	0C:11:05:0B:00:6D
Firmware Version	20.30.4.8
Hardware Version	20.9.0.0.0.0.0.0

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.