

## **About This Manual**

Thank you for choosing Akuvox E16C door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to 116.30.1.134 version, and it provides all the configurations for the functions and features of E16C door phones. Please visit Akuvox forum or consult technical support for any new information or the latest firmwares.

# Introduction of Icons and Symbols



## Warning:

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



## Caution:

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



## Note:

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



## Tip:

- Useful information for the quick and efficient use of the device.

# Related Documentation

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

**<https://knowledge.akuvox.com>**



### **FCC Caution:**

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

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

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

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

#### **FCC Radiation Exposure Statement:**

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

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

# Table of Contents

|  |    |
|--|----|
| 1. Product Overview .....                                    | 1  |
| 2. Change Log .....  | 2  |
| 3. Introduction to Configuration Menu .....                  | 3  |
| 4. Access the Device .....                                   | 4  |
| 4.1. Access the Device Setting on the device .....           | 5  |
| 4.2. Access the Device Setting on the Web Interface .....    | 5  |
| 5. Time and Language Setting .....                           | 6  |
| 5.1. Language Setting .....                                  | 7  |
| 5.2. Time Setting .....                                      | 7  |
| 5.3. LED Setting .....                                       | 8  |
| 5.3.1. Configure Card Reader LED Setting .....               | 8  |
| 5.3.2. Configure LED White Light Setting .....               | 9  |
| 5.4. Screen Display configuration .....                      | 10 |
| 5.4.1. Configure Screensaver .....                           | 10 |
| 5.4.2. Upload Screensaver .....                              | 11 |
| 5.5. Volume & Tone Configuration .....                       | 12 |
| 5.5.1. Volume Configuration .....                            | 12 |
| 5.5.2. Upload Open Door Tone .....                           | 13 |
| 5.5.3. Configure Door Access Prompt Text .....               | 13 |
| 6. Network Setting .....                                     | 14 |
| 6.1. Device Network Connection Setting .....                 | 14 |
| 6.2. Device Deployment in Network .....                      | 15 |
| 6.3. NAT Setting .....                                       | 16 |
| 7. Intercom Call Configuration .....                         | 17 |
| 7.1. IP call & IP Call Configuration .....                   | 17 |
| 7.1.1. Make IP calls .....                                   | 17 |
| 7.1.2. IP Call Configuration .....                           | 18 |
| 7.2. SIP Call & SIP Call Configuration .....                 | 18 |
| 7.2.1. SIP Account Registration .....                        | 19 |
| 7.2.2. SIP Server Configuration .....                        | 20 |
| 7.2.3. Configure Outbound Proxy Server .....                 | 20 |
| 7.2.4. Configure Data Transmission Type .....                | 21 |
| 7.3. Call Auto-answer Configuration .....                    | 22 |
| 7.4. Call Settings .....                                     | 23 |
| 7.4.1. Maximum Call Duration Setting .....                   | 23 |
| 7.4.2. Maximum Dial Duration Setting .....                   | 23 |
| 7.4.3. Audio & Video Codec Configuration for SIP Calls ..... | 24 |
| 7.4.3.1. Configure Audio Codec .....                         | 24 |

|   |    |
|---|----|
| 7.4.3.2. Configure Video Codec .....                                  | 25 |
| 7.5. Configure DTMF Data Transmission .....                           | 26 |
| 8. Relay Switch Setting .....   | 27 |
| 8.1. Relay Switch Setting .....                                       | 27 |
| 8.2. Web Relay Setting .....  | 28 |
| 8.2.1. Configure Web Relay on the Web Interface .....                 | 28 |
| 8.2.2. Configure Web Relay on the Device .....                        | 30 |
| 9. Door Access Schedule Management .....                              | 31 |
| 9.1. Configure Door Access Schedule .....                             | 31 |
| 9.1.1. Create Door Access Schedule .....                              | 31 |
| 9.1.2. Import and Export Door Access Schedule .....                   | 32 |
| 9.1.3. Edit the Door Access Schedule .....                            | 33 |
| 10. Door Unlock Configuration .....                                   | 34 |
| 10.1. Configure PIN Code for Door Unlock .....                        | 34 |
| 10.1.1. Configure Public PIN code .....                               | 34 |
| 10.1.2. Configure Private PIN Code on the Device .....                | 35 |
| 10.1.3. Configure Private PIN Code on the Web Interface .....         | 36 |
| 10.1.4. Configure Private PIN Access Mode .....                       | 37 |
| 10.2. Configure RF Card for Door Unlock .....                         | 38 |
| 10.2.1. Configure RF Card on the Web Interface .....                  | 38 |
| 10.2.1.1. Configure RF Card Code Format .....                         | 39 |
| 10.2.2. Configure Facial Recognition for Door Unlock .....            | 39 |
| 10.2.2.1. Configure Facial Recognition on the Device .....            | 39 |
| 10.2.2.2. Configure Facial Recognition on Web Interface .....         | 40 |
| 10.3. Configure Door Access Using Configured Files. ....              | 41 |
| 10.4. Editing the User(s)-specific door access data .....             | 41 |
| 10.4.1. Unlock by QR Code .....                                       | 42 |
| 10.4.2. Unlock by Bluetooth .....                                     | 42 |
| 10.4.3. Unlock by HTTP Command on Web Browser .....                   | 43 |
| 10.4.4. Unlock by Exit Button by the Door .....                       | 44 |
| 10.4.5. Unlock by Reception Tab .....                                 | 45 |
| 10.4.6. Unlock by DTMF Code .....                                     | 46 |
| 10.4.7. Body Temperature Measurement for Door Access (Optional) ..... | 47 |
| 10.4.7.1. Body Temperature Measurement Configuration .....            | 47 |
| 10.4.7.2. Ambient Temperature Configuration .....                     | 49 |
| 11. Security .....  | 50 |
| 11.1. Tamper Alarm Setting .....                                      | 50 |
| 11.2. Security Notification Setting .....                             | 51 |
| 11.2.1. Email Notification Setting .....                              | 51 |
| 11.2.2. FTP Notification setting .....                                | 52 |
| 11.2.3. TFTP Notification Setting .....                               | 53 |
| 11.3. Web Interface Automatic Log-out .....                           | 53 |
| 12. Monitor and Image .....   | 54 |
| 12.1. MJPEG Image Capturing .....                                     | 54 |

|   |    |
|---|----|
| 12.2. Live Stream .....                               | 55 |
| 12.3. RTSP Stream Monitoring .....                    | 56 |
| 12.3.1. RTSP Basic Setting .....                      | 56 |
| 12.3.2. RTSP Stream Setting .....                     | 57 |
| 12.4. ONVIF .....                                     | 58 |
| 13. Logs .....  | 60 |
| 13.1. Call Logs .....                                 | 60 |
| 13.2. Door Logs .....                                 | 60 |
| 13.3. Temperature Log .....                           | 61 |
| 14. Debug .....                                       | 62 |
| 14.1. System Log for Debugging .....                  | 62 |
| 14.2. PCAP for Debugging .....                        | 63 |
| 15. Firmware Upgrade .....                            | 64 |
| 16. Backup .....                                      | 65 |
| 17. Auto-provisioning via Configuration File .....    | 66 |
| 17.1. Provisioning Principle .....                    | 66 |
| 17.2. Configuration Files for Auto-provisioning ..... | 67 |
| 17.3. AutoP Schedule .....                            | 67 |
| 17.4. DHCP Provisioning Configuration .....           | 68 |
| 17.5. Static Provisioning Configuration .....         | 70 |
| 18. Integration with Third Party Device .....         | 73 |
| 18.1. Integration via Wiegand .....                   | 73 |
| 18.2. Integration via RS485 .....                     | 74 |
| 18.3. OSDP Setting .....                              | 75 |
| 19. Password Modification .....                       | 77 |
| 20. System Reboot&Reset .....                         | 78 |
| 20.1. Reboot .....                                    | 78 |
| 20.2. Reset .....                                     | 79 |
| 21. Abbreviations .....                               | 80 |
| 22. Contact Us .....                                  | 82 |

# 1. Product Overview

Akuvox E16C 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. E16C 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. E16C 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. 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.

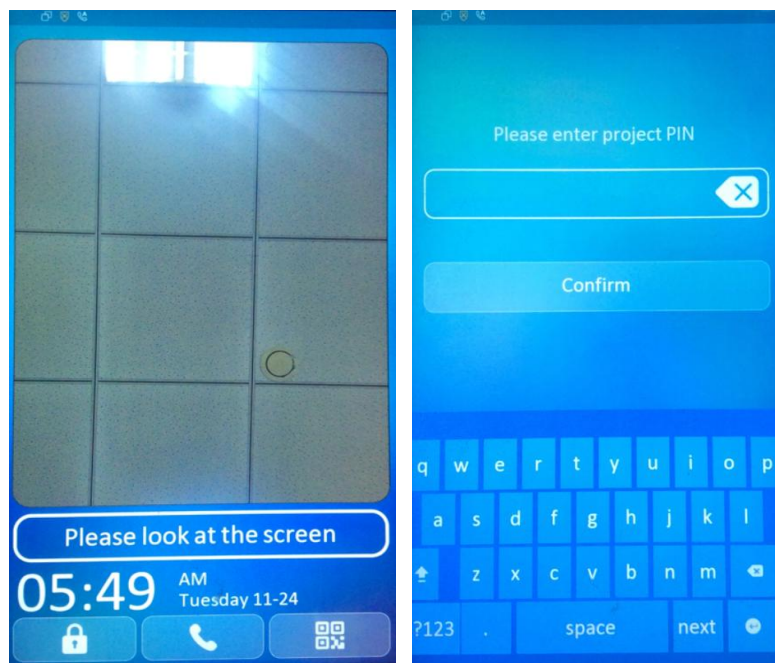
1. **SDMC:** SDMC is suitable for the management of Akuvox devices large communities, including access control, resident information, remote device control etc.,.
2. **Akuvox Upgrade tool:** Upgrade Akuvox devices in batch on a LAN (**Local Area Network**).
3. **Akuvox PC Manager:** Distribute all configuration 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.

## 4. Access the Device

E16C door phone system setting can be either accessed on the device directly or on the device web interface.

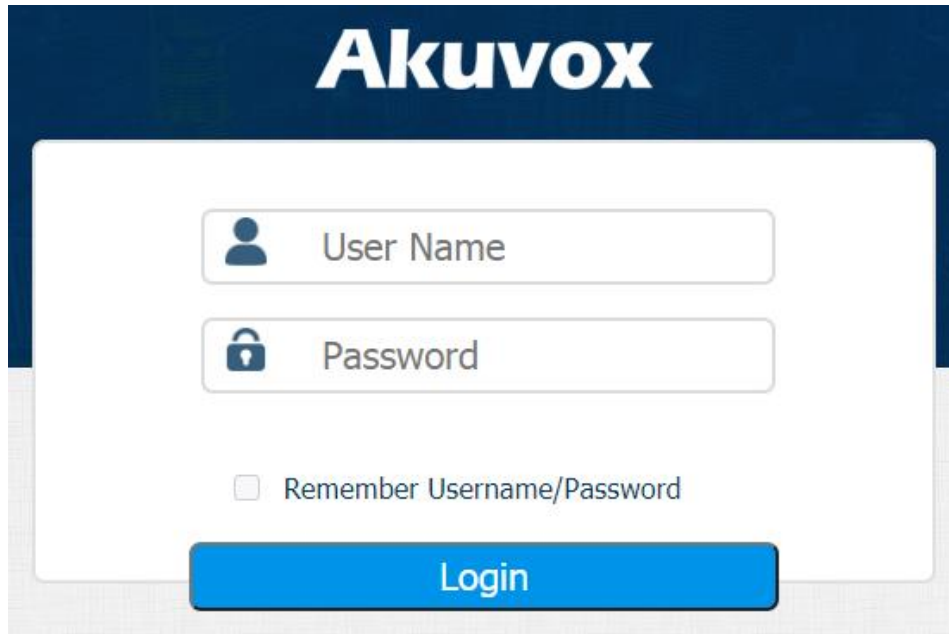
## 4.1. Access the Device Setting on the device

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



## 4.2. Access the Device Setting on the Web Interface

You can also use Akuvox IP scanner tool to search the device IP address in the same LAN. Then 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. Then use the IP address to login in the web browser by user name and password **admin** and **admin**.



**Akuvox**

User Name

Password

Remember Username/Password

Login

✓ **Tip:**

- You can also obtain the device IP address using the Akuvox IP scanner to log in the device web interface. Please refer to the URL below for the IP scanner application:  
[http://wiki.akuvox.com/doku.php?id=tool:ip\\_scanner&s\[\]=ip&s\[\]=scanner](http://wiki.akuvox.com/doku.php?id=tool:ip_scanner&s[]=ip&s[]=scanner)

! **Note:**

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

## 5. Time and Language Setting

## 5.1. Language Setting

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 **Setting > Time/Lang > LCD Language** interface.

## 5.2. Time Setting

Time setting on the web **Setting > Time/Lang > Time** interface allows you to set up time and date manually while allowing you to use 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.

### 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:**

- When the check box is not ticked, the parameters related to NTP server will become unedited.

## 5.3. LED Setting

### 5.3.1. Configure Card Reader LED Setting

You can enable or disable the LED lighting on the card reader area as needed on the web interface. Meanwhile, If you do not want 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 configure the configuration on web **Setting > Time/Lang > Time** Interface.

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

**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).

### 5.3.2. 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. To configure the configuration on web **Device > Light > White Light** interface.

| White Light   |                                   |
|---|-----------------------------------|
| Mode  | <input type="text" value="Auto"/> |
| Max White Light Value   | <input type="text" value="3"/>    |
| <input type="button" value="Submit"/> <input type="button" value="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 can be valid in the facial recognition, however IR LED light does not need to be triggered for the white light function in the QR code scan.

## 5.4. Screen Display configuration

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

### 5.4.1. Configure Screensaver

Await screen is mainly a function for 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. To configure the configuration on web **Device > LCD > Standby Interface Display** interface.

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.

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

**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"/> | <span style="background-color: #f44336; color: white; padding: 2px 5px;">Delete 🗑</span> |
| 2              | File Exists | <input type="text" value="5"/> | <span style="background-color: #f44336; color: white; padding: 2px 5px;">Delete 🗑</span> |
| 3              | File Exists | <input type="text" value="5"/> | <span style="background-color: #f44336; color: white; padding: 2px 5px;">Delete 🗑</span> |
| 4              | File Exists | <input type="text" value="5"/> | <span style="background-color: #f44336; color: white; padding: 2px 5px;">Delete 🗑</span> |
| 5              | File Exists | <input type="text" value="5"/> | <span style="background-color: #f44336; color: white; padding: 2px 5px;">Delete 🗑</span> |

Submit
Cancel

## 5.5. Volume & Tone Configuration

Volume and tone configuration in E16C 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.

### 5.5.1. 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 go to **Device > Voice > Volume Control** interface.

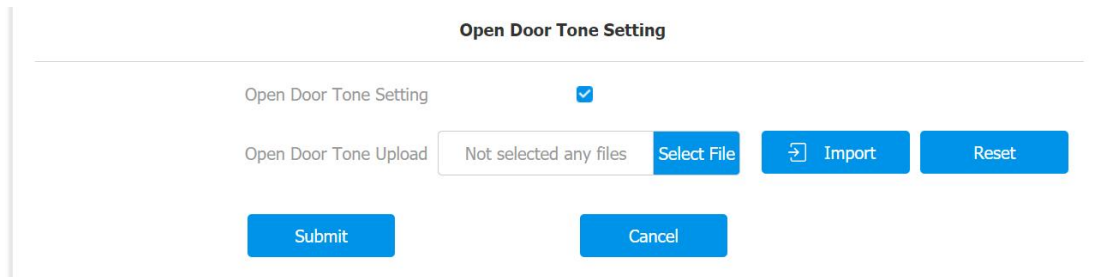
| Light                 | Wiegand             | RS485                          | Voice  | LCD |
|-----------------------|---------------------|--------------------------------|--------|-----|
| <b>Volume Control</b> |                     |                                |        |     |
|                       | 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) |     |

#### Parameter Set-up:

- **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".

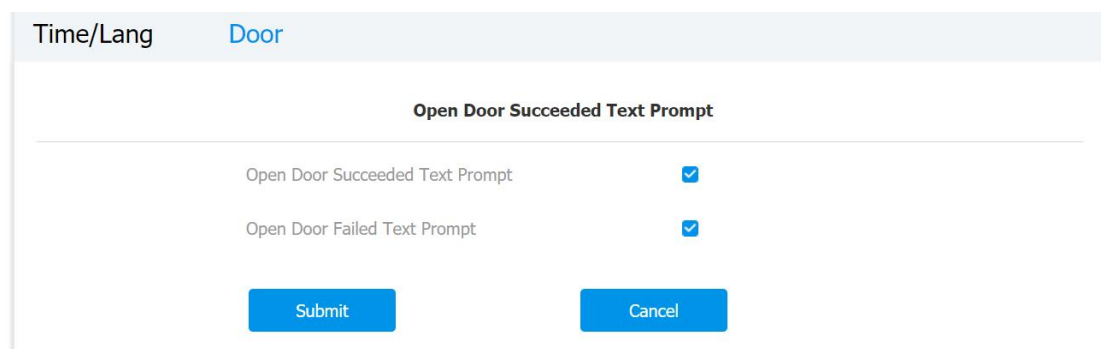
### 5.5.2. Upload Open Door Tone

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



### 5.5.3. Configure Door Access Prompt Text

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



**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.

## 6. Network Setting

### 6.1. Device Network Connection Setting

You can configure the default DHCP mode (**Dynamic Host Configuration Protocol**) and static IP connection. Moreover, you can set up IP address, Subnet Mask, Default Gateway, LAN DNS1 & LAN DNS2. To configure the configuration on web **Network > Ethernet > LAN Port** interface.

The screenshot shows the 'Ethernet' configuration page, specifically the 'LAN Port' sub-section. It features two radio buttons: 'DHCP' (checked) and 'Static IP' (unchecked). Below these are five input fields: 'IP Address' (192.168.1.100), 'Subnet Mask' (255.255.255.0), 'Default Gateway' (192.168.1.1), 'LAN DNS1' (8.8.8.8), and 'LAN DNS2' (empty). At the bottom, there are 'Submit' and 'Cancel' buttons.

#### 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 .

## 6.2. Device Deployment in Network

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

### Parameter Set-up:

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

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

## 6.3. NAT Setting

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 **Account > Advanced > NAT** interface.



### Parameter Set-up:

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



## 7. Intercom Call Configuration

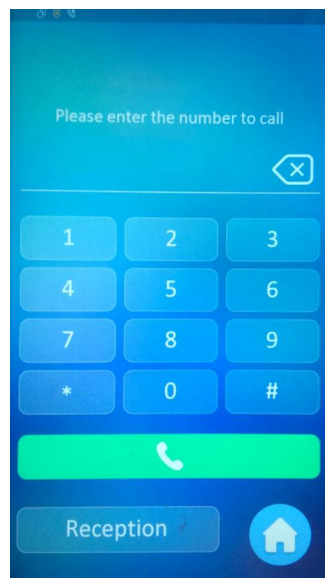
Intercom call in the device can be configured to allow you to perform a variety of customized intercom calls such as IP call and SIP call for different application scenarios.

### 7.1. 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.

#### 7.1.1. Make IP calls

To make directly IP call on the device, you can press the dial  icon, then enter the IP or SIP number and press the **Call**  icon to call out.





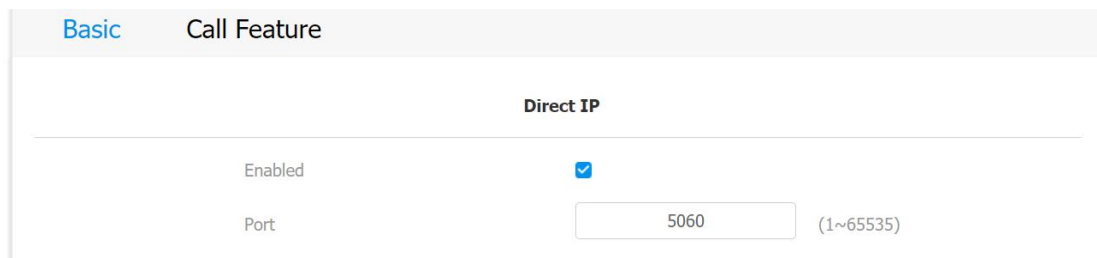


**Note:**

- You can press **Home**  on the **Dial** screen if you want to go back to the initial screen.

## 7.1.2. IP Call Configuration

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



**Parameter Set-up:**

- **Direct IP Call:** go to **“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 go to **“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.

## 7.2. 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.

## 7.2.1. SIP Account Registration

E16C 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 **Account > Basic > SIP Account** Interface.

### Parameter Set-up:

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

## 7.2.2. SIP Server Configuration

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

The screenshot displays the configuration page for SIP servers. It is divided into two main sections: 'Preferred SIP Server' and 'Alternate SIP Server'. Each section contains three input fields: 'Server IP' (empty), 'Registration Period' (set to 1800), and 'Port' (set to 5060). The 'Port' field is labeled 'Port' and has a small box next to it containing the value 5060.

### Parameter Set-up:

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

## 7.2.3. Configure Outbound Proxy Server

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

**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"/> |

Submit
Cancel

**Parameter Set-up:**

- **Enable Outbound:** go to “**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.

### 7.2.4. 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 go to **Account > Basic > Transport Type**.

**TransportType**

---

|               |                                  |
|---------------|----------------------------------|
| TransportType | <input type="text" value="UDP"/> |
|---------------|----------------------------------|

**Parameter Set-up:**

- **UDP:** select “UDP” for unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
- **TCP:** select “TCP” for 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 servers. And **SRV** not only records the server address but also the server port. Moreover, SRV can also be used to configure the priority and the weight of the server address.

### 7.3. 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 go to **Account > Advanced > Call to Enable or Disable in Auto Answer** and Set up auto-answer delay time.

The screenshot shows a configuration page titled "Call". It has two main sections: "Call" and "Auto Answer".

- Call Section:**
  - Auto Answer:** A dropdown menu currently set to "Disabled".
  - Auto Answer Delay:** A text input field containing the value "0".
- Auto Answer Section:**
  - Auto Answer Delay:** A text input field containing "0" with a range indicator "(0~5 Sec)" to its right.
  - Mode:** A dropdown menu currently set to "Audio".

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

**Parameter Set-up:**

- **Auto Answer:** turn on the the Auto Answer function by go toing “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.

## 7.4. Call Settings

### 7.4.1. Maximum Call Duration Setting

E16C 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 go to **Intercom > Call Feature > Max Call Time**.

#### 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.

### 7.4.2. 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 go to **Intercom > Call Feature> Max Dial Time**.

**Max Dial Time**

---

|               |   |              |
|---------------|---|--------------|
| Dial In Time  | <input style="width: 80%;" type="text" value="60"/> | (30~120 Sec) |
| Dial Out Time | <input style="width: 80%;" 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.

### 7.4.3. Audio & Video Codec Configuration for SIP Calls

#### 7.4.3.1. Configure Audio Codec

E16C 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 go to **Account > Advanced > Audio Codecs**.

**Audio Codecs**

---

|  |  |   |  |
|--|--|---|--|
| Disabled Codecs  |  | Enabled Codecs  |  |
| <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> | <input type="button" value=" &gt;&gt;"/><br><input type="button" value=" &lt;&lt;"/> | <div style="border: 1px solid #ccc; padding: 5px;">                     PCMU<br/>                     PCMA<br/>                     G729<br/>                     G722                 </div> | <input type="button" value=" ↑"/><br><input type="button" value=" ↓"/> |

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

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

### 7.4.3.2. Configure Video Codec

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

Video Codecs

|            |   |
|------------|---|
| Name       | <input checked="" type="checkbox"/> H264  |
| Resolution | 720P <span style="float: right;">▼</span> |
| Bitrate    | 2048 <span style="float: right;">▼</span> |
| Payload    | 104 <span style="float: right;">▼</span>  |

#### Parameter Set-up:

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



- **Payload:** select the payload type (ranging from 90-118) to configure the audio codec payload. The pay load between the door phone and the corresponding intercom device should be identical. The default payload is 104.

## 7.5. 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 go to **Account > Advanced > DTMF**.

| 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.

## 8. Relay Switch Setting

### 8.1. Relay Switch Setting

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

| Relay              |              |
|--------------------|--------------|
| Trigger Delay(Sec) | 0            |
| Hold Delay(Sec)    | 5            |
| DTMF Mode          | 1 Digit DTMF |
| 1 Digit DTMF       | 0            |
| 2~4 Digits DTMF    |              |
| Relay Status       | Relay: High  |
| Relay Name         | Relay        |

#### Parameter Set-up:

- **Trigger Delay (Sec):** set the relay trigger delay timing (Ranging from 1-10 Sec.) For example, if you set the delay time as "5" sec. then the relay will not triggered until 5 seconds after you press "unlock " tab.
- **Hold Delay (Sec):** set the relay hold delay timing (Ranging from 1-10 Sec.) For example, if you set the hold delay time as " 5" Sec. then the relay will be delayed for 5 after the door is unlocked.
- **DTMF Mode:** select the number of DTMF digit for the door access control (Ranging from 1-4 digits ) For example, you can select 1 digit DTMF code or 2-digit DTMF code etc., according to your need.
- **1-digit DTMF :** set the 1-digit DTMF code within range from ( 0-9 and \*,#).
- **2~4 Digits DTMF:** set the DTMF code according to the **DMTP Option** setting. For example, you are required to set the 3-digits DTMF code if

**DTMP Mode** is set as 3-digits.

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



**Note:**

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



**Note:**

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

## 8.2. 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.

### 8.2.1. 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 configure the configuration on web **Access Control > Web Relay** interface.

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 style="width: 150px;" type="text"/> | <input style="width: 100px;" type="text"/> | <input style="width: 100px;" type="text"/> |
| Action ID 02 | <input style="width: 150px;" type="text"/> | <input style="width: 100px;" type="text"/> | <input style="width: 100px;" type="text"/> |
| Action ID 03 | <input style="width: 150px;" type="text"/> | <input style="width: 100px;" type="text"/> | <input style="width: 100px;" type="text"/> |

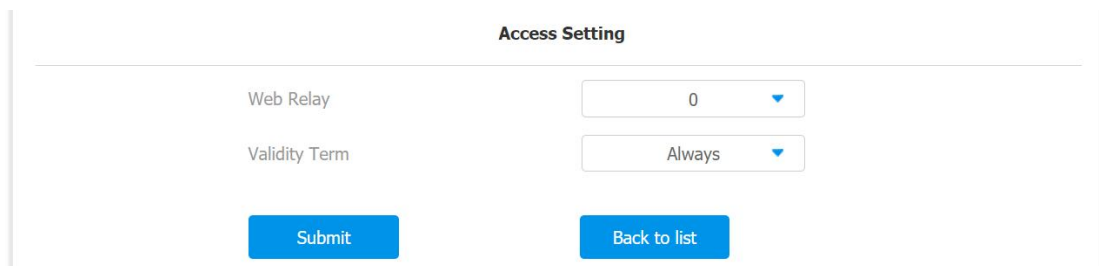
**Parameter Set-up:**

- **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:

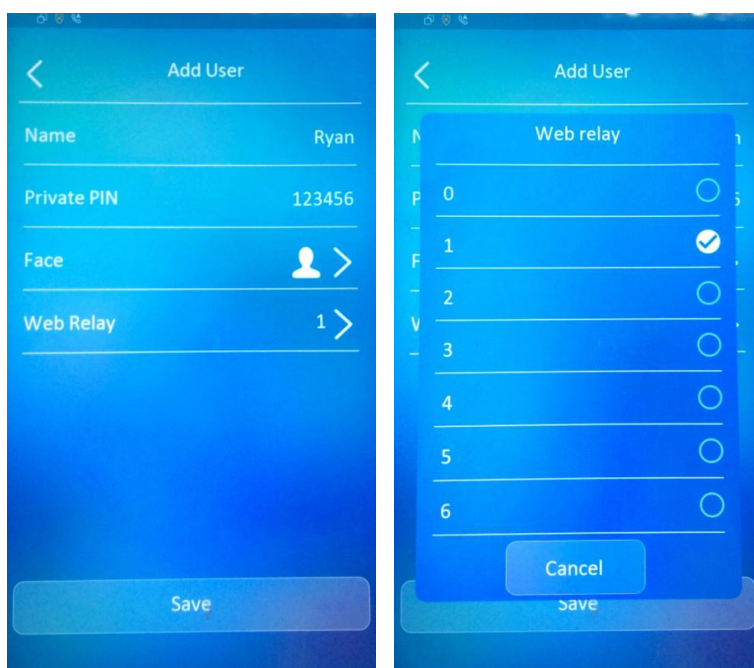
<http://admin:admin@192.168.1.2/state.xml?relayState=2>.

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 configuration on web **Access Control > User** interface.



### 8.2.2. 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 device **User > Setting** screen. Firstly, press **User**  then press **Add** tab. Secondly, Press Web Relay arrow  and tick the circle  icon to assign the specific web relay to a resident. Finally press the **Save** tab on the **Add User** screen for the validation.



## 9. 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.

### 9.1. 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.

#### 9.1.1. 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 configure the configuration on web **Access Control > Schedule Setting** interface.

**Schedule Setting**

---

Schedule Type: Daily

Schedule Name:

Date Time: 00 : 00 - 00 : 00

+ Add
Reset

To create a weekly schedule, select **Schedule Type** as **Weekly**.

**Schedule Setting**

---

Schedule Type: Weekly

Schedule Name:

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

Date Time: 00 : 00 - 00 : 00

+ Add
Reset

To create a longer period schedule, select **Schedule Type** as **Normal**.

### 9.1.2.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 configure the configuration on web **Access Control > Schedule Setting > Import/Export Schedule(.xml)** interface.

**Note:**

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

### 9.1.3. 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 configure the configuration on web **Access Control > Schedule Setting > Schedule Management** interface.

**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



## 10. Door Unlock Configuration

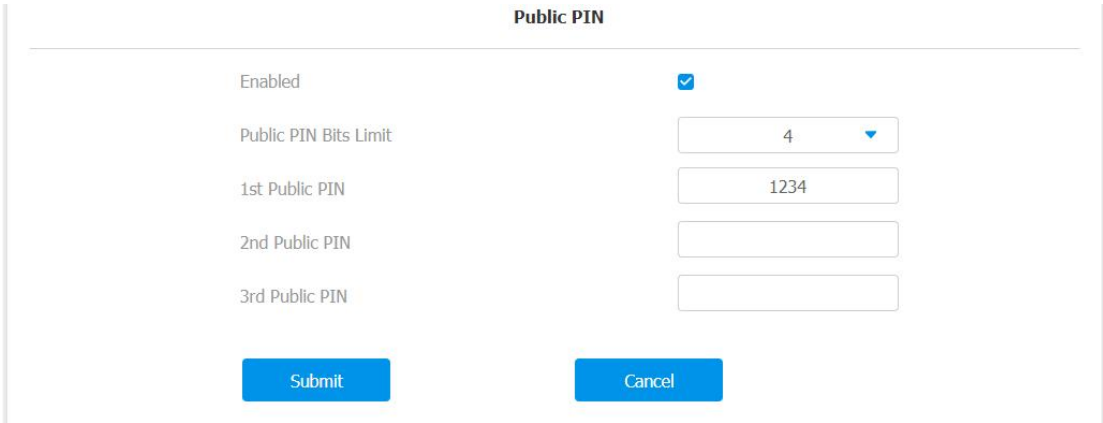
E16C door phone offer you three types of door access via PIN code, RF card and Facial recognition. You can configure them on the device and web interface. More over, you can import or exporting the configured files to maximize your RF card configuration efficiency.

### 10.1. Configure PIN Code for Door Unlock

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

#### 10.1.1. Configure Public PIN code

You can configure and modify a total of 3 sets of separate PIN codes on the device web **Access Control > PIN Setting > Public PIN** interface. Tick the check box to enable the public PIN code then set the PIN code digit limit ranging from "4-8" in Public PIN Bits Limit field and Enter the Public PIN codes.



The screenshot shows the 'Public PIN' configuration page. It includes a title bar 'Public PIN' and a form with the following fields and controls:

- Enabled:** A checkbox that is checked.
- Public PIN Bits Limit:** A dropdown menu currently set to '4'.
- 1st Public PIN:** A text input field containing '1234'.
- 2nd Public PIN:** An empty text input field.
- 3rd Public PIN:** An empty text input field.
- Submit:** A blue button at the bottom left.
- Cancel:** A blue button at the bottom right.

**Note:**


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

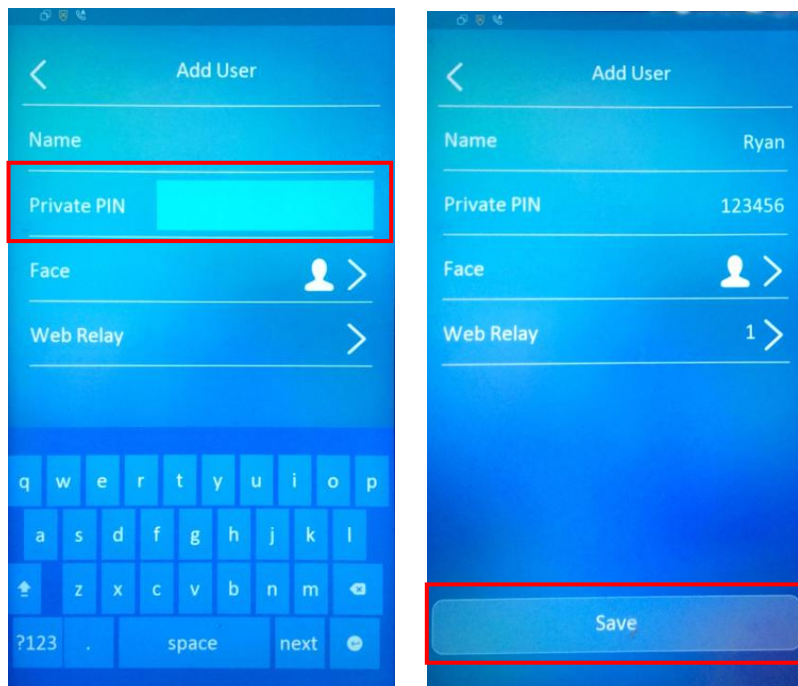
**Note:**

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

### 10.1.2. 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 press **User**  icon on the **Setting** screen. Press **Add** tab and enter the User name. Then enter the private PIN in the **Private PIN** field.



### 10.1.3. Configure Private PIN Code on the Web Interface

On the web **Access Control > User** 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. Enter the **user's name** and **floor number** then go to **Private PIN** section to enter the private PIN code in **Code**.

The screenshot shows the 'User' configuration page. At the top, there are tabs for 'Input', 'Relay', 'Web Relay', 'Door Log', 'Face Setting', and 'CardSetting'. The 'User' tab is selected. Below the tabs, there are sub-sections: 'User Basic' with fields for 'Name' (Ryan) and 'Floor No.' (403), and 'Private PIN' with a 'Code' field (123456).

To select door access Schedule for Private PIN Code door access, you can go to **Access Setting** interface to Set up PIN code validity time in the **Validity Term** field and set the limit for the total number. Then select targeted user(s).

The screenshot shows the 'Access Setting' page. A red box highlights the 'Validity Term' dropdown menu (set to 'Schedule'), the 'Frequency' dropdown menu, and the 'All Schedules' section. The 'All Schedules' section contains two lists of schedules: '1:Daily (Work Hour) Time', '2:Weekly Cleaning', and '3:Day Shift'. There are navigation buttons '>>' and '<<' between the lists, and 'Submit' and 'Back to list' buttons at the bottom.

**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.

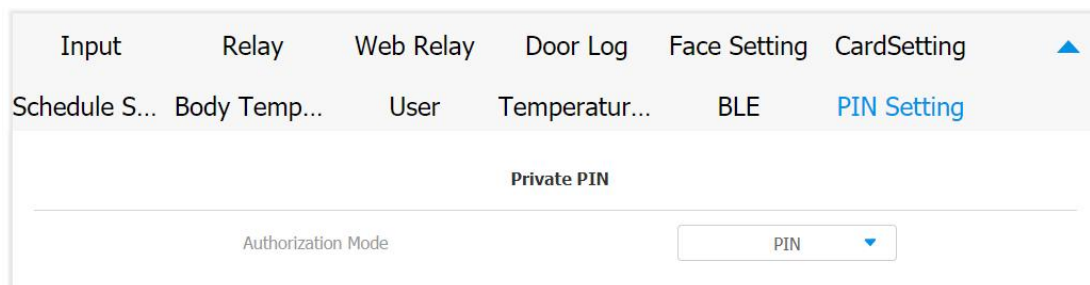


**Note:**

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

### 10.1.4. Configure Private PIN Access Mode

E16C 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 go to **Access Control > PIN Setting > Private PIN** to select **Authorization Mode**.



**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.

## 10.2. Configure RF Card for Door Unlock

### 10.2.1. Configure RF Card on the Web Interface

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

RF Card

Card

**Note:**

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

**Note:**

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

### 10.2.1.1. 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 configure the configuration on web **Access Control > CardSetting** interface.

The screenshot shows a web interface for configuring RF card settings. At the top, there is a navigation bar with tabs: Input, Relay, Web Relay, Door Log, Face Setting, and CardSetting (which is highlighted in blue). Below this is a sub-menu with options: Schedule S..., Body Temp..., User, Temperatur..., BLE, and PIN Setting. The main content area is titled 'RFID' and contains a section for 'IC-Card Display Mode'. A dropdown menu is currently set to '8HN'. At the bottom of this section are two blue buttons: 'Submit' and 'Cancel'.


#### Parameter Set-up:

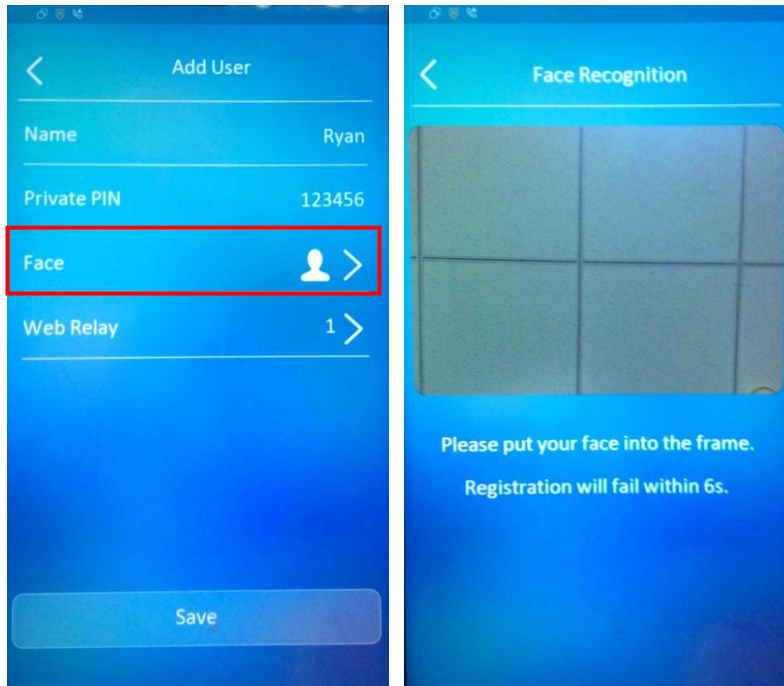
- **IC-Card Display Mode:** select the card format for the ID Card for the door access among five format options: **8H10D**; **6H3D5D(W26)**; **6H8D**; **8HN**; **8HR**. The card code format is 8HN by default in the door phone.

### 10.2.2. Configure Facial Recognition for Door Unlock

#### 10.2.2.1. Configure Facial Recognition on the Device

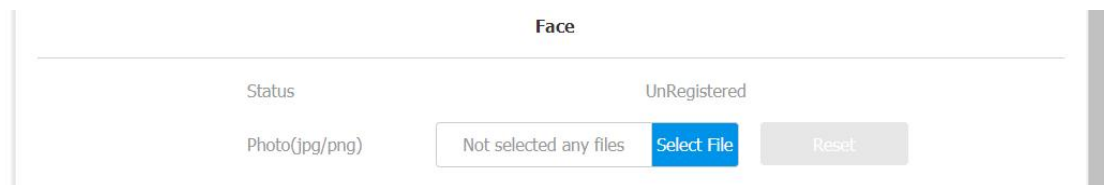
To configure the facial recognition, you can configure door access by facial recognition on the device by entering the user's name and register your facial ID on the device for the door access.

To configure facial recognition, you can press **User**  on **Setting** screen. Press **Add** and enter the **User name**. Click on **Face** for facial recognition then 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.



### 10.2.2.2. Configure Facial Recognition on Web Interface

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



#### Parameter Set-up:

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



**Note:**

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

## 10.3. Configure Door Access Using Configured Files.

E16C door phones allow you to speedily configure user(s)-specific door access in batch by importing the configured all-in-one door access control files incorporating user information, door access type, door access schedule etc., thus all the door access 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 configure the configuration on web **Access Control > User** interface.

**Import/Export User**

|                        |                        |                             |                        |                        |                       |
|------------------------|------------------------|-----------------------------|------------------------|------------------------|-----------------------|
| User Data(Except Face) | Not selected any files | <a href="#">Select File</a> | <a href="#">Import</a> | <a href="#">Export</a> |                       |
| Face                   | Not selected any files | <a href="#">Select File</a> | <a href="#">Import</a> | <a href="#">Export</a> | <a href="#">Reset</a> |



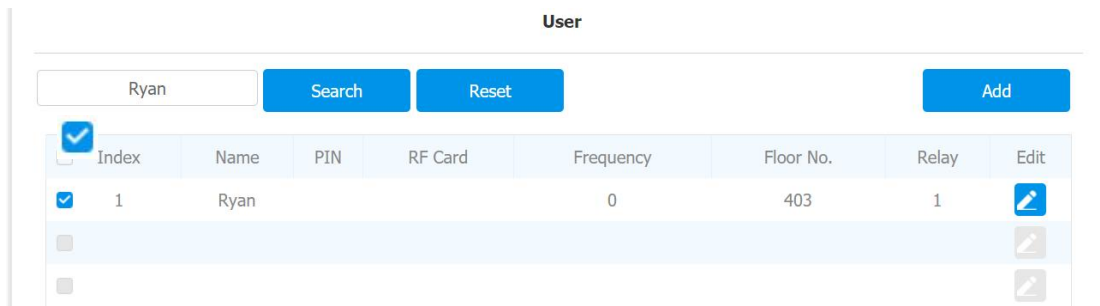
**Note:**

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

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

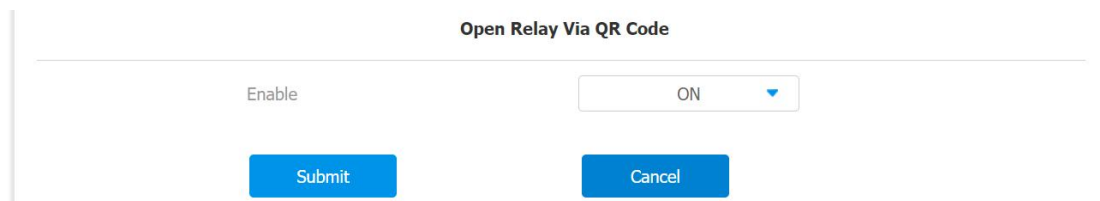
You can search user(s)-specific door access and edit the door access data on the web **Access Control > User** interface.





### 10.4.1. 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 go to **Access Control > Relay > Open Relay via QR Code**.



**Note:**

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

### 10.4.2. 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 access control terminal for the door access. To configure the configuration on web **Access Control > BLE > BLE** interface.

**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.

### 10.4.3. 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 configure the configuration on web **Access Control > Relay > Open Relay via HTTP** interface.

**Parameter Set-up:**

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

Please refer to the following example:

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

**Note:**

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

## 10.4.4. 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 access control terminal Input to trigger the relay for the door access. To configure the configuration on web **Access Control > Input > Input** interface.

**Parameter Set-up:**

- **Trigger Electrical Level:** select the trigger electrical level options between “High” and “Low” according the actual operation on the exit button.
- **Execute Relay:** set up relays to be triggered by the input.
- **Door Status:** display the status of input signal.

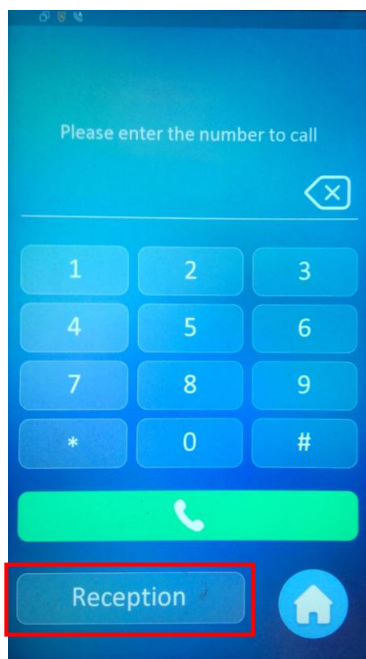
## 10.4.5. Unlock by Reception Tab

In the device home screen, E16C 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 go to **Intercom > Basic > Key Setting**.

**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.



### 10.4.6. 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 go to **Account > Advanced > DTMF** interface.

| DTMF               |                         |
|--------------------|-------------------------|
| Type               | RFC2833 <span>▼</span>  |
| How To Notify DTMF | Disabled <span>▼</span> |
| DTMF Payload       | 101 (96~127)            |

**Parameter Set-up:**

- **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 Transmission** for the specific DTMF code setting.
- Intercom devices involved must be consistent in the DTMF type otherwise DTMF code cannot be applied.

## 10.4.7. Body Temperature Measurement for Door Access (Optional)

E16C 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.

### 10.4.7.1. 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 configure the configuration on web **Access Control > Body Temperature > Measuring Body Temperature** interface.

Input    Relay    Web Relay    Door Log    Face Setting    CardSetting    ▲

Schedule S...    **Body Temp...**    User    Temperatur...

---

**Measuring Body Temperature**

---

|   |                                       |
|---|---------------------------------------|
| Mode  | Disabled ▼                            |
| Mask Detection  | Disabled ▼                            |
| Temperature Unit  | Centigrade ▼                          |
| Normal Body Temperature   | 37.3 (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   | <input type="checkbox"/> SIP/ IP Call |
| SIP/ IP Call Number   | <input type="text"/>                  |

**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 are 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.

### 10.4.7.2. 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 configure the configuration on web **Access Control > Body Temperature > Ambient Temperature Setting** interface.

**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°C degree 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 .



# 11. Security

## 11.1. 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 configure the configuration on web **Security > Basic > Temper Alarm** interface.

| Tamper Alarm |   |
|--------------|---|
| Enable       | <input checked="" type="checkbox"/> <span>Disarm</span> |
| Key Status   | Low   |

### Parameter Set-up:

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

#### **Note:**

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

#### **Note:**

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

## 11.2. Security Notification Setting

### 11.2.1. Email Notification Setting

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

| Time/Lang                 | Action                   | Door                     |
|---------------------------|--------------------------|--------------------------|
| <b>Email Notification</b> |                          |                          |
|                           | 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"/> |
|                           | 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.

### 11.2.2. 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 configure the configuration on web **Setting > Action > FTP Notification** interface.

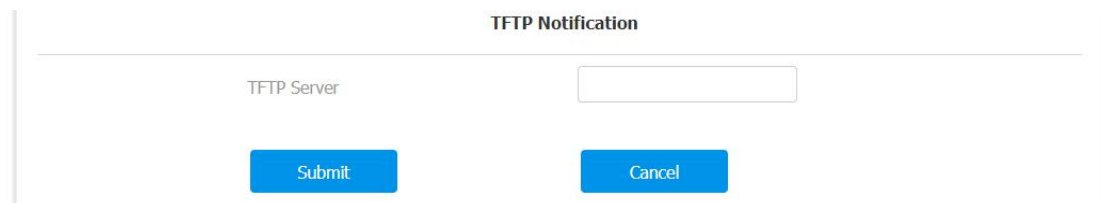
| FTP Notification |  |
|------------------|--|
| FTP Server       | <input type="text"/>                   |
| FTP User Name    | <input type="text"/>                   |
| FTP Password     | <input type="password" value="*****"/> |
| FTP Path         | <input type="text"/>                   |

#### 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.

### 11.2.3. 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 configure the configuration on web **Setting > Action > TFTP Notification** interface.



TFTP Notification

TFTP Server

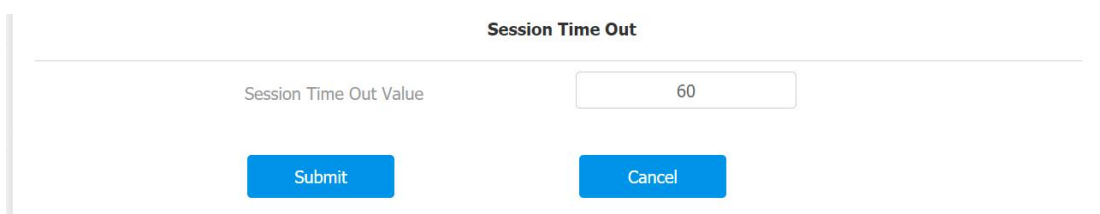
Submit Cancel

#### Parameter set-up:

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

### 11.3. Web Interface Automatic Log-out

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



Session Time Out

Session Time Out Value

Submit Cancel

## 12. Monitor and Image

### 12.1. MJPEG Image Capturing

E16C 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 configure the configuration on web **Surveillance > MJPEG > MJPEG Server** interface.

#### 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**

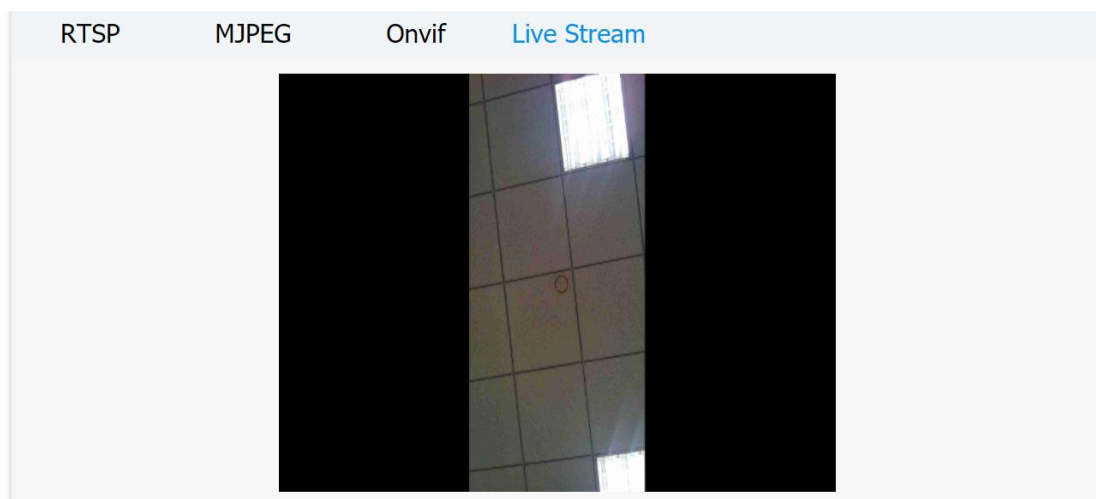
After the MJPEG service is enabled, you can capture the image from the door phone using following three types of URL format:

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

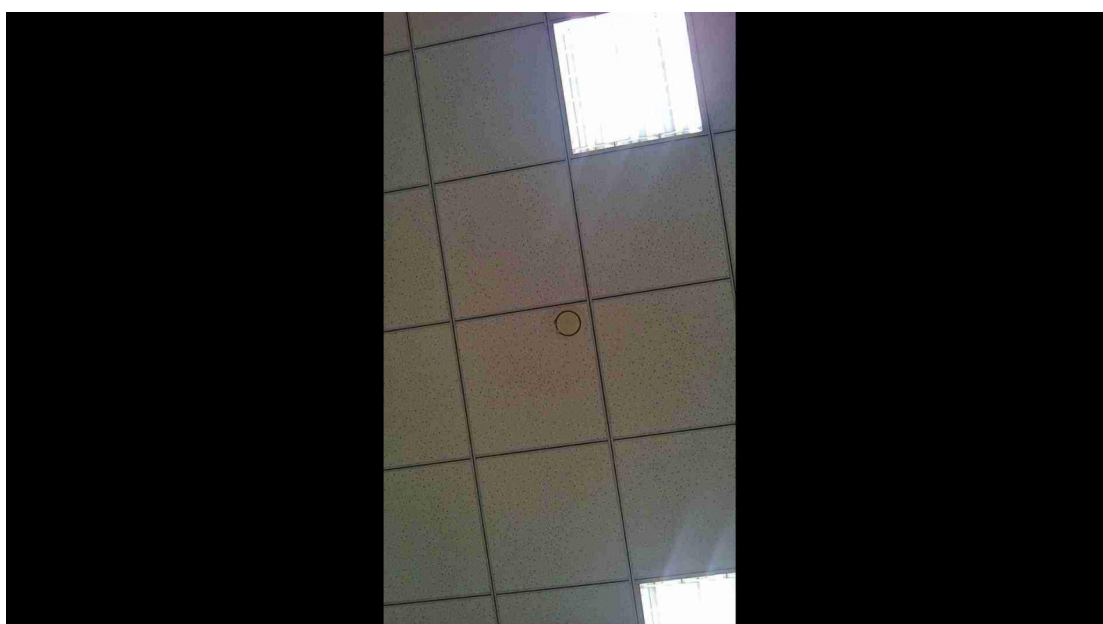
For example, if you want to capture the jpg format image of door phone with the IP address: 192.168.1.104, you can Enter "http://192.168.1.104:8080/picture.jpg" on the web browser.

## 12.2.Live Stream

If you want to check the real-time video from the E16C access control terminal, you can go to the device web interface to obtain the real-time video or you can also enter the correct URL on the web browser to obtain it directly. To see the live stream on web **Surveillance > Live Stream** interface.



To check the real time video using URL, you can Enter the correct URL ([http://IP\\_address:8080/video.cgi](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 > Check the real time video.

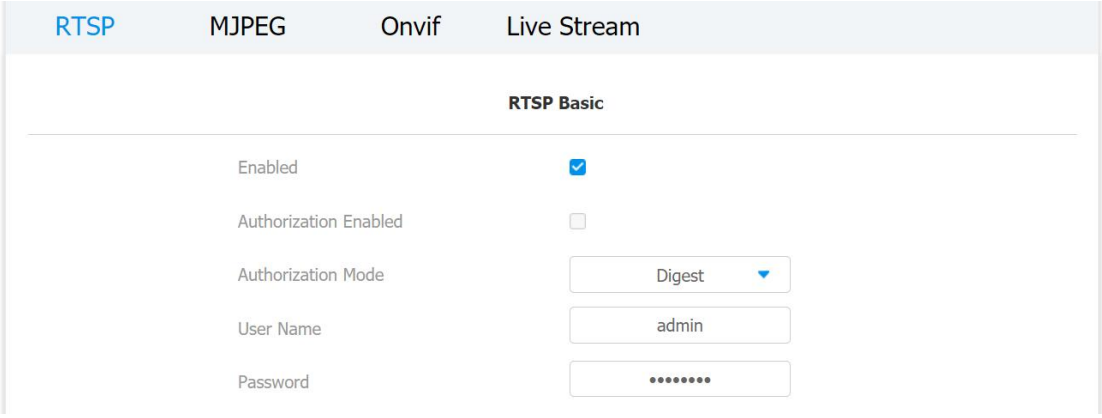


## 12.3. RTSP Stream Monitoring

E16C 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.

### 12.3.1. 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 configure the configuration on web **Surveillance > RTSP > RTSP Basic** interface.



| RTSP                  | MJPEG                               | Onvif | Live Stream |
|-----------------------|-------------------------------------|-------|-------------|
| <b>RTSP Basic</b>     |                                     |       |             |
| Enabled               | <input checked="" type="checkbox"/> |       |             |
| Authorization Enabled | <input type="checkbox"/>            |       |             |
| Authorization Mode    | Digest ▼                            |       |             |
| User Name             | admin                               |       |             |
| Password              | .....                               |       |             |

#### Parameter Set-up:

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

### 12.3.2. RTSP Stream Setting

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

**H.264 Video Parameters**


|                      |           |
|----------------------|-----------|
| Video Resolution     | 1080P     |
| Video Framerate      | 25 fps    |
| Video Bitrate        | 4096 kbps |
| 2nd Video Resolution | VGA       |
| 2nd Video Framerate  | 25 fps    |
| 2nd Video Bitrate    | 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 kbps" according to your network environment. The default video bit-rate is "2048 kbps".
- **2nd Video Resolution2:** select video resolution for the second video stream channel. While the default video solution is "VGA".
- **2nd Video Framerate:** select the video framerate for the second video stream channel. "25fps" is the video frame rate by default for the second video stream channel.



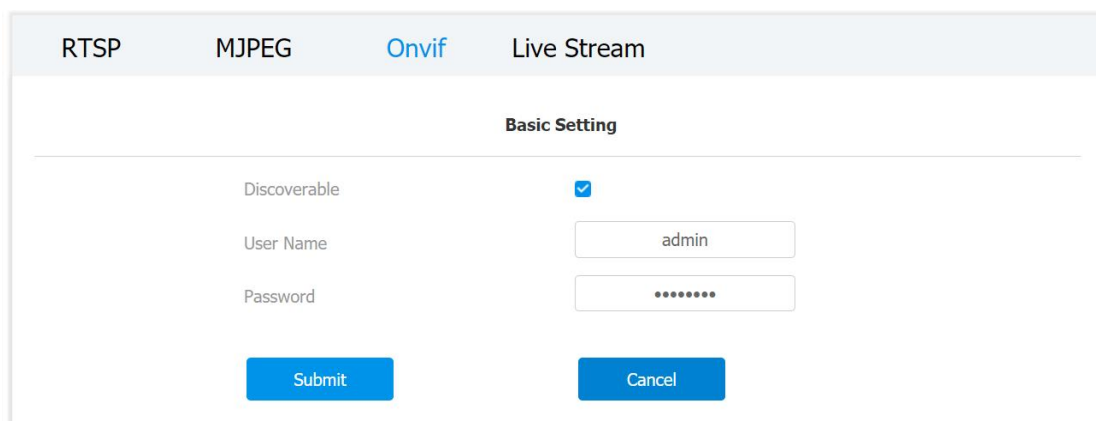
- **2nd Video Bitrate:** select video bit-rate among the six options for the second video stream channel. While the second video stream channel is "512 kpbs" by default.

 **Note:**

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

## 12.4. ONVIF

Real-time video from the E16C access control terminal 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 access control terminal so that other device will be able to see the video from the access control terminal. To configure the configuration on web **Intercom > ONVIF** interface.



### Parameter Set-up:

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

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

For example: **http://IP address:80/onvif/device\_service**

**Note:**

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

# 13. Logs

## 13.1. Call Logs

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

| Index                                 | Type   | Date       | Time     | Local Identity    | Name           | Number                            |
|---------------------------------------|--------|------------|----------|-------------------|----------------|-----------------------------------|
| <input type="checkbox"/>              |        |            |          | 192.168.35.1      |                | <a href="#">192.168.35.1</a>      |
| <input checked="" type="checkbox"/> 1 | Dialed | 2020-11-24 | 06:47:07 | 14@192.168.35.114 | Indoor Monitor | <a href="#">26@192.168.35.126</a> |
| <input type="checkbox"/> 2            | Dialed | 2020-11-24 | 06:46:46 | 14@192.168.35.114 | Indoor Monitor | <a href="#">26@192.168.35.126</a> |
| <input type="checkbox"/> 3            | Dialed | 2020-11-24 | 06:46:13 | 14@192.168.35.114 | Indoor Monitor | <a href="#">26@192.168.35.126</a> |

### 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.

## 13.2. 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 **Access > Door log** interface.

Input Relay Web Relay **Door Log** Face Setting CardSetting

Save Door Log Enabled

All Time mm/dd/yyyy - mm/dd/yyyy Name/Code Search Export

| <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 | <a href="#">View</a> |
| <input type="checkbox"/> 2            | Ryan | 0745983600 | Card | 2020-11-13 | 08:25:09 | Success | <a href="#">View</a> |
| <input type="checkbox"/> 3            | Ryan | 0745983600 | Card | 2020-11-13 | 08:24:23 | Success | <a href="#">View</a> |

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.

### 13.3. Temperature Log

To check temperature log on web **Access Control > Temperature Log** interface.

Input Relay Web Relay Door Log Face Setting CardSetting

Schedule S... Body Temp... User **Temperature Log**

Status All

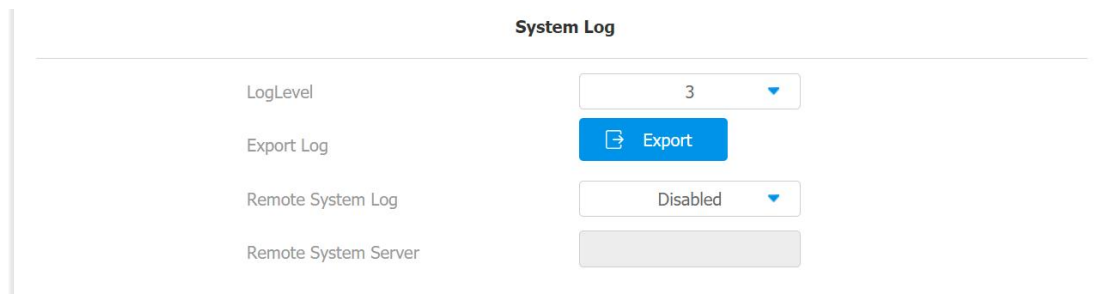
Time mm/dd/yyyy - mm/dd/yyyy Filter Export

| <input type="checkbox"/> Index | Temperature | Status | Date | Time | Picture |
|--------------------------------|-------------|--------|------|------|---------|
| <input type="checkbox"/> 1     |             |        |      |      |         |
| <input type="checkbox"/> 2     |             |        |      |      |         |
| <input type="checkbox"/> 3     |             |        |      |      |         |

## 14. Debug

### 14.1. System Log for Debugging

System log in the access control terminal 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 **Upgrade > Advanced > System Log** interface.



| System Log           |          |
|----------------------|----------|
| 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:** go to 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.

## 14.2.PCAP for Debugging

PCAP in E16C access control terminal 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 **Upgrade > Advanced > PCAP** interface properly before using it.

### Parameter set-up:

- **Specific Port:** select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** go to **Start** tab and **Stop** tab to capture the a certain range of data packets before go toing **Export** tab to export the data packets to you Local PC.
- **PCAP Auto Refresh:** select "**Enable**" or "**Disable**" to turn on or turn off the PCAP auto fresh function. If you set it as " Enable" then the PCAP will continue to capture data packet even after the data packets reached its 1M maximum in capacity. If you set it as "**Disable**" the PCAP will stop data packet capturing when the data packet captured reached the maximum capturing capacity of 1MB.

## 15. Firmware Upgrade

Firmware of different versions for E16C access control terminal can be upgraded on the device web **Upgrade > Basic** interface.

| Basic                    | Advanced  |
|--------------------------|---|
| Firmware Version         | 116.30.0.28   |
| Hardware Version         | 116.0.5.1.0.0.0.0   |
| Upgrade                  | <input type="text" value="Not selected any files"/> <input type="button" value="Select File"/><br><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"/>   |

 **Note:**

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

## 16. Backup

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

The screenshot shows the 'Others' section of a web interface. At the top, it says 'Others'. Below that, there is a file selection area with the text 'Config File(.tgz/.conf/.cfg)' on the left and a box containing 'Not selected any files' and a 'Select File' button on the right. Below the file selection area, there are four buttons: 'Import' (with a folder icon), 'Export (Encrypted)' (with a folder icon), 'Submit', and 'Cancel'.

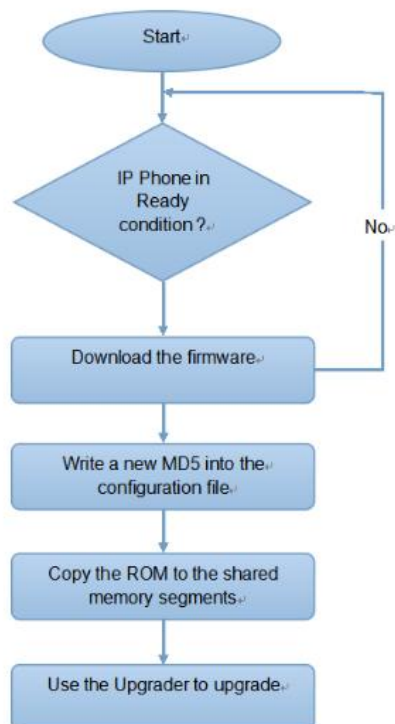


# 17. Auto-provisioning via Configuration File

Configurations and upgrading on E16C door phone can be done on the web interface via one-time auto-provisioning and scheduled auto-provisioning via configuration files, thus saving you from setting up configuration needed one by one manually on the door phone.

## 17.1. 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 update the firmware and the corresponding parameters on the door phone.



## 17.2. 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 devices will first access the general configuration files before accessing the MAC-based configuration files.

## 17.3.AutoP Schedule

Akuvox provides you with different Autop methods that enable the access control terminal to perform provisioning for itself in a specific time according to your schedule. To configure the configuration on web **Upgrade > Advanced > Automatic Autop** interface.

**Automatic Autop**

Mode: Power On

Schedule: Sunday

Hour(0~23): 22    Min(0~59): 0

Clear MD5    Submit

Export Autop Template    Export

**Parameter Set-up:**

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

## 17.4.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, on web **Upgrade > Advanced > Automatic Autop** interface. Click **Export** tab in **Export Autop Template** to export Autop template. Then set up DHCP Option on DHCP server.

**Automatic Autop**

---

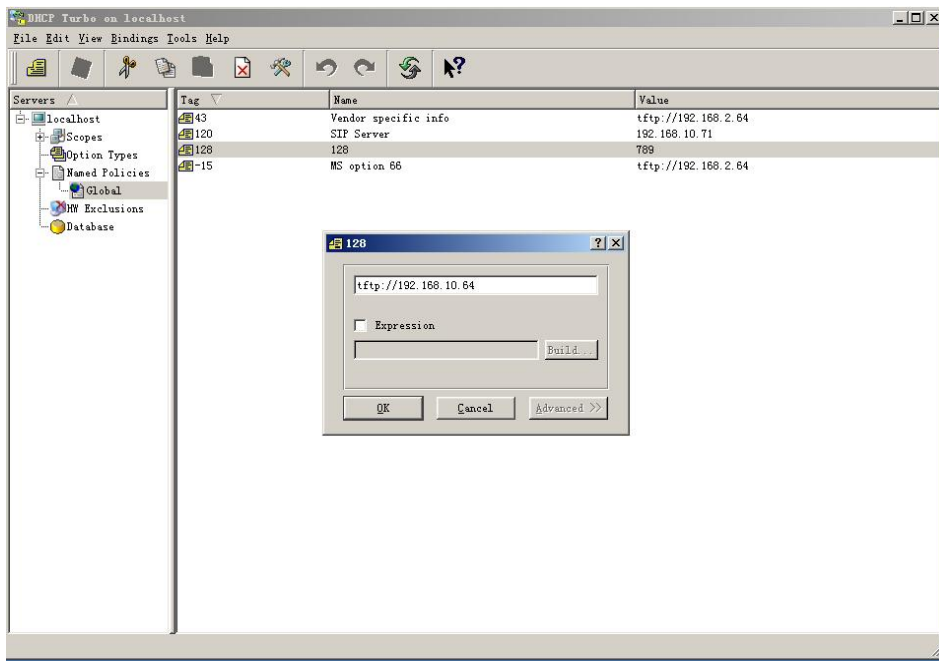
Mode Power On ▼

Schedule Sunday ▼

22 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 of TFTP server.

**DHCP Option**

---

Custom Option  (128~254)

(DHCP Option 66/43 is Enabled by Default)

**Parameter set-up:**

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

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

**Note:**

- The general configuration file for the in-batch provisioning is with the format "r0000000000xx.cfg" taking E16C as an example "r000000000016.cfg ( 10 "zeros" in total while the MAC-based configuration file for the specific device provisioning is with the format "MAC\_Address of the device.cfg, for example "0C110504AE5B.cfg."

## 17.5.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 access control terminal will perform the auto provisioning on a specific timing according to autop schedule you set up. In addition, TFTP, FTP, HTTP, and HTTPS are the protocols that can be used for upgrading the device firmware and configuration. To download the Autop template on **Upgrade > Advanced > Automatic Autop** , and setup Autop server on **Upgrade > Advanced > Manual Autop** interface.

**Automatic Autop**

---

Mode Power On ▾

Schedule Sunday ▾

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

Clear MD5

Export Autop Template

**Manual Autop**

---

URL

User Name

Password

Common AES Key

AES Key(MAC)

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:**

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

**Note:****Server Address format:**

- TFTP: tftp://192.168.0.19/
- FTP: ftp://192.168.0.19/ (allows anonymous login)
- ftp://username:password@192.168.0.19/(requires a user name and password)
- HTTP: http://192.168.0.19/ (use the default port 80)
- http://192.168.0.19:8080/ (use other ports, such as 8080)
- HTTPS: https://192.168.0.19/ (use the default port 443)

**Tip:**

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

# 18. Integration with Third Party Device

## 18.1. Integration via Wiegand

If you want to integrate the E16C access control terminal with the third-party devices via Wiegand, you can configure the Wiegand on the web **Device > Wiegand > Wiegand** interface.

### Parameter Set-up:

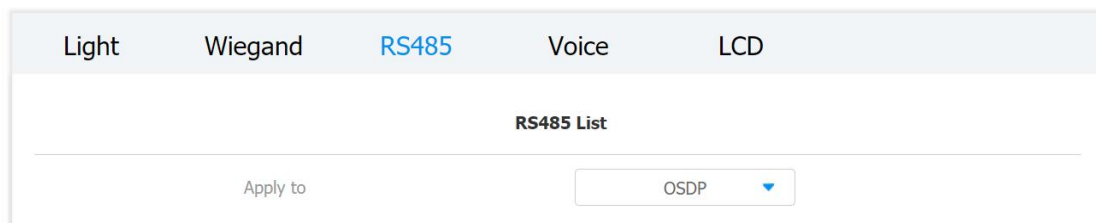
- **Wiegand Display Mode:** select Wiegand Card code format among **8H10D**; **6H3D5D**; **6H8D**; **8HN**; **8HR**; **RAW**.
- **Wiegand Card Reader Mode:** set the wiegand data transmission format among three options: **Wiegand 26**, **Wiegand 34**, **Wiegand 58**. The transmission format should be 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.

## 18.2. Integration via RS485

RS485 integration mode should be configured properly on the access control terminal's web interface before you can implement the integration between the access control terminal and the third-party devices. To configure the configuration on web **Device > RS485 > RS485 List** interface.



### Parameter Set-up:

- **RS485 List:** select integration mode between two options: " **None** ," **OSDP**", the detail for the two options will be provided in the following chart.

| NO. | Integration Mode | Description  |
|-----|------------------|--|
| 1   | None             | If you select "None" then the RS485 integration will be disabled.  |
| 2   | OSDP             | If you Select "OSDP" Mode, then the integration communication between the E16C door phone and the third party device is via OSDP protocol. You are required to check for the device integration protocol and make sure if that they use the same integration protocol. |

### 18.3. 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 configure the configuration on web **Device > RS485 > OSDP Advance Setting** interface.

**Parameter Set-up:**

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

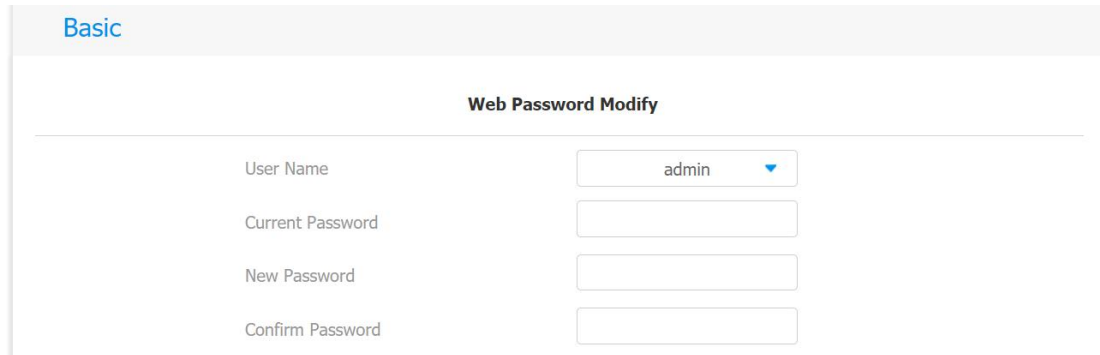
the system.

**Note:**

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

## 19. Password Modification

On the device web interface, you can set and change password for accessing the web **Security > Basic > Web Password Modify** interface. In addition, you can also select the user role when setting passwords.



The screenshot shows the 'Basic' section of the web interface. Under the heading 'Web Password Modify', there are four input fields: 'User Name' (a dropdown menu currently showing 'admin'), 'Current Password', 'New Password', and 'Confirm Password'.

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

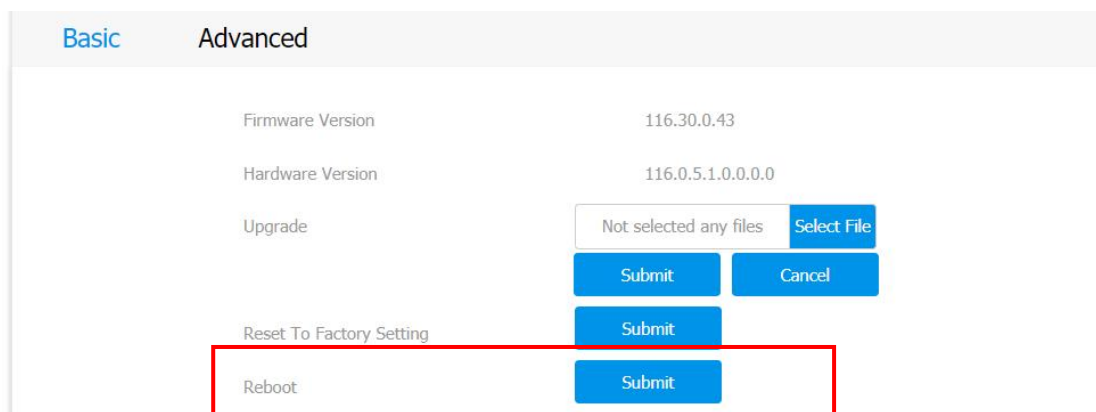


The screenshot shows the 'Project PIN' section of the web interface. It contains a single input field labeled 'Code' with a masked PIN (represented by seven dots).

## 20. System Reboot&Reset

### 20.1.Reboot

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

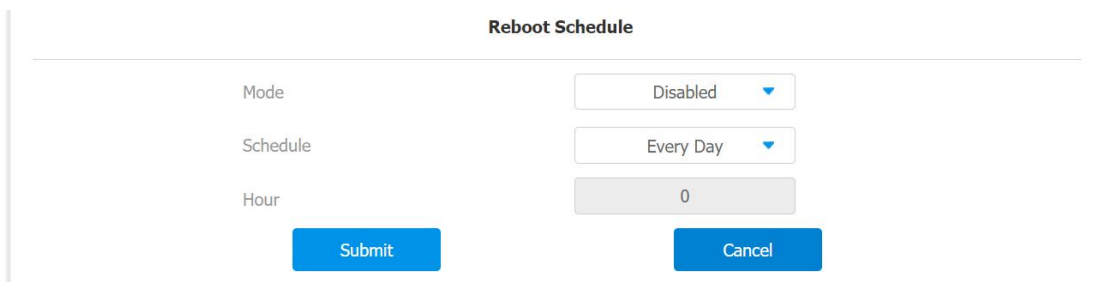


The screenshot shows the 'Basic' tab of the system configuration interface. It displays the following information:

|                          |   |
|--------------------------|---|
| 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"/>                                       |

The 'Reboot' row is highlighted with a red rectangular border.

To set up the device restart schedule on web **Upgrade > Advanced > Reboot Schedule** interface.



The screenshot shows the 'Reboot Schedule' configuration interface with the following settings:

|          |   |
|----------|---|
| Mode     | Disabled  |
| Schedule | Every Day   |
| Hour     | 0   |
|          | <input type="button" value="Submit"/> <input type="button" value="Cancel"/> |

## 20.2.Reset

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

The screenshot shows the 'Basic' tab of the web interface. It contains the following elements:

- Basic** (selected) and **Advanced** tabs.
- Firmware Version**: 116.30.0.43
- Hardware Version**: 116.0.5.1.0.0.0.0
- Upgrade**: A file selection area with the text "Not selected any files", a **Select File** button, and **Submit** and **Cancel** buttons.
- Reset To Factory Setting**: A button highlighted with a red border, with a **Submit** button next to it.
- Reboot**: A **Submit** button.

## 21. Abbreviations

**ACS:** Auto Configuration Server

**Auto:** Automatically

**AEC:** Configurable Acoustic and Line Echo Cancelers

**ACD:** Automatic Call Distribution

**Autop:** Automatical Provisioning

**AES:** Advanced Encryption Standard

**BLF:** Busy Lamp Field

**COM:** Common

**CPE:** Customer Premise Equipment

**CWMP:** CPE WAN Management Protocol

**DTMF:** Dual Tone Multi-Frequency

**DHCP:** Dynamic Host Configuration Protocol

**DNS:** Domain Name System

**DND:** Do Not Disturb

**DNS-SRV:** Service record in the Domain Name System

**FTP:** File Transfer Protocol

**GND:** Ground

**HTTP:** Hypertext Transfer Protocol

**HTTPS:** Hypertext Transfer Protocol Secure Socket Layer

**IP:** Internet Protocol

**ID:** Identification

**IR:** Infrared

**LCD:** Liquid Crystal Display

**LED:** Light Emitting Diode

**MAX:** Maximum

**POE:** Power Over Ethernet

**PCMA:** Pulse Code Modulation A-Law

**PCMU:** Pulse Code Modulation  $\mu$ -Law

**PCAP:** Packet Capture

**PNP:** Plug and Play

**RFID:** Radio Frequency Identification

**RTP:** Real-time Transport Protocol

**RTSP:** Real Time Streaming Protocol

**MPEG:** Moving Picture Experts Group

**MWI:** Message Waiting Indicator

**NO:** Normal Opened

**NC:** Normal Connected

**NTP:** Network Time Protocol

**NAT:** Network Address Translation

**NVR:** Network Video Recorder

**ONVIF:** Open Network Video Interface Forum

**SIP:** Session Initiation Protocol

**SNMP:** Simple Network Management Protocol

**STUN:** Session Traversal Utilities for NAT

**SMTP:** Simple Mail Transfer Protocol

**SDMC:** SIP Devices Management Center

**TR069:** Technical Report069

**TCP:** Transmission Control Protocol

**TLS:** Transport Layer Security

**TFTP:** Trivial File Transfer Protocol

**UDP:** User Datagram Protocol

**URL:** Uniform Resource Locator

**VLAN:** Virtual Local Area Network

**WG:** Wiegand



## 22. Contact Us

For more information about the product, please visit us at [www.akuvox.com](http://www.akuvox.com) or feel free to contact us by

Sales email: [sales@akuvox.com](mailto:sales@akuvox.com)

Technical support email: [support@akuvox.com](mailto:support@akuvox.com)

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

We highly appreciate your feedback about our products.

