R28 Series Door Phone Admin Guide

About This Manual

Thank you for choosing Akuvox's R28 series door phone. This manual is intended for end users who need to properly configure the door phone. This manual is applicable to 28.31.1.xx version, and it provides all functions' configurations of R28 series door phone. Please visit Akuvox forum or consult technical support for any new information or latest firmware.

Note: Please refer to universal abbreviation form in the end of manual when meet any abbreviation letter.

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.

Content

1.

1.Product Overview

1.1. Instruction

R28 series is an Linux-based doorphone and SIP-compliant with a 4.3'' screen and a dialpad. It incorporates audio communications, camera capabilities and access control.

It is applicable to multi-storey residential buildings, high-rise office buildings and their complexes.

Occupants can communicate with visitors via audio and video calls, and unlock the door if they need. Visitors can also use PIN codes or RFID cards to unlock the door.

Its multiple ports, Door, Relay(COM), RS485 and Wiegand, can be used to easily integrate external digital systems, such as elevator controller and fire alarm detector, creating a holistic entrance control.

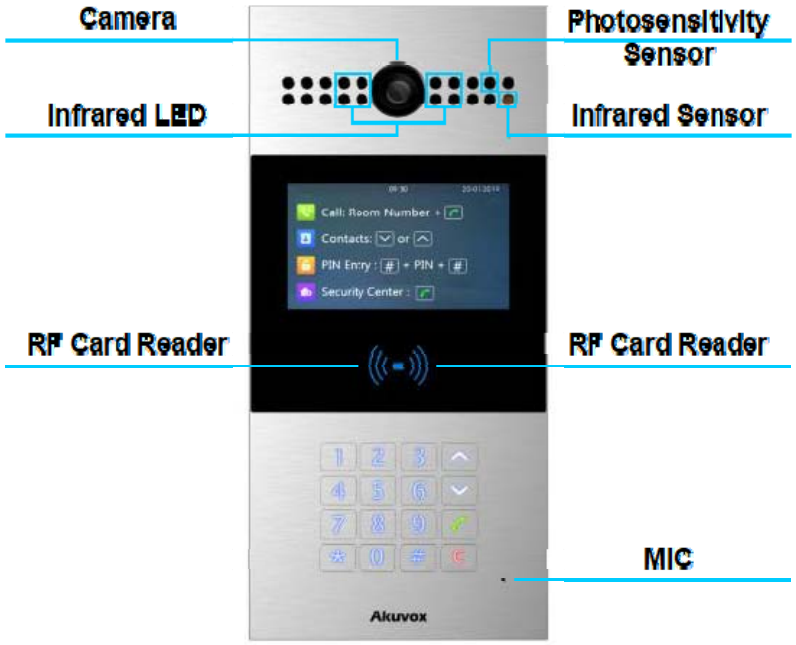

Figure1.1 Product Description

1.2Connector Introduction

Ethernet (POE): Ethernet (POE) connector which it can provide both power and network connection.

12V/GND: External power supply terminal if POE connector is not available.

WG_D0/WG_D1: Wiegand terminal.

DOORA/B/C: Trigger signal input terminal.

RS485A/B: RS485 terminal.

RelayA/B/C (NO/NC/COM): Relay control terminal.

12V_OUT/GND_OUT: External power output terminal.

Note: The general door phone interface diagram is only for reference.

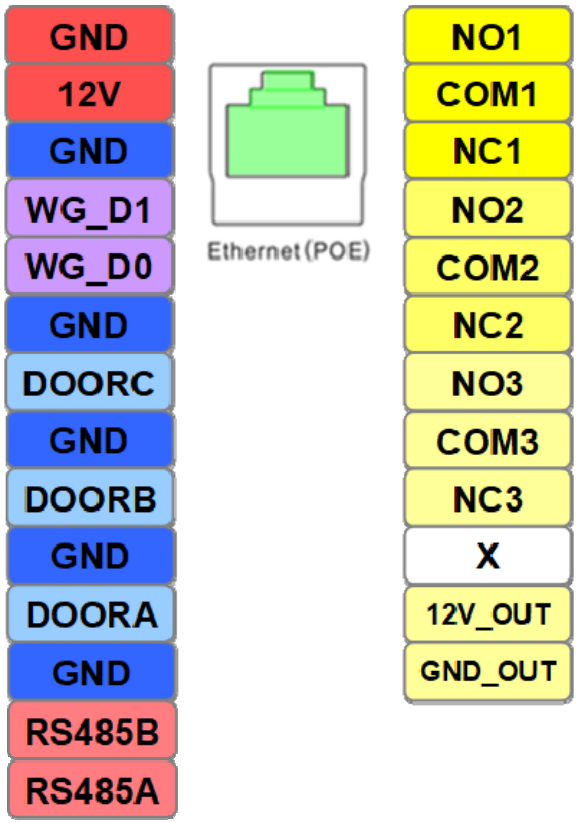

Figure 1.2-1 R28's interface

2. Daily Use

2.1. Make a Call

Visitors can make a call in the main interface.

2.1.1. Dial

Dial The room number/sip account or ip address and press  to call

2.1.2. Contacts

Press  or  to select a contact, and press  to call.

2.1.3. Security Center

Press  directly, to call for security center.

2.2. Receive a Call

It will auto answer the incoming call by default. If users disable auto answer function, they can press “Dial key” to answer the

incoming call.

2.3. Unlock

2.3.1. Unlock by PIN Codes

Press # PIN Code # to unlock, then visitors will hear “The door is now opened” and the screen will show “Unlock”. If visitors input the wrong PIN code, the screen will show “Incorrect PIN”.

2.3.2. Unlock by RF cards

The Building-in card reader supports 13.56MHz and 125kHz RFID-Card .

Place a registered card on RF area to unlock., then visitors will hear “The door is now opened” and the screen will show “Unlock”. If the card has not been registered, the phone will show “Invalid Card”.

2.3.3. Unlock by DTMF codes

During the calling, the Occupants can press the predefined DTMF codes to remote unlock the door. then visitors will hear “The door is now opened” and the screen will show “Unlock”.

3.Basic Features

3.1.Access Settings

3.1.1.Administrator Interface

Press “*2396#” to enter administrator interface. Administrator interface provides some advanced permissions to administrators, including “System Information,” “Admin Settings” and “System Settings.”

3.2.Access the Website Setting

3.2.1.Obtain IP Address

R27 use DHCP IP by default. Press “*2396#” to enter administrator interface. Press “1” to enter system Information interface to check the IP address.

3.2.2.Access the Device Website

Open a web browser, and access the corresponding IP address. Enter the default user name and password to login. The default

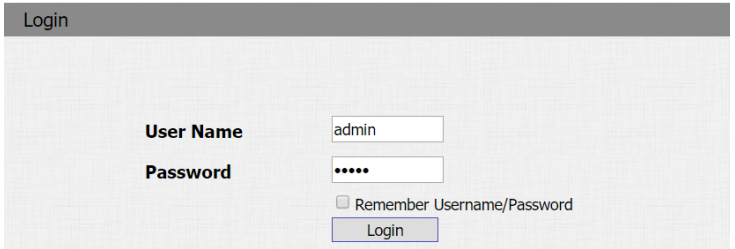

Figure 3.2.2 Access the device website

administrator’s user name and password are shown below:

User Name: **admin**

Password: **admin**

Note: The recommended browser is Google Chrome.

3.3.Password Modification

3.3.1.Admin Password Settings on R28

Go to **Settings - Admin Settings - Admin Password Setting** on R28,to modify Admin Password on R28.

3.3.2.Modify the Device Service Code

Service code is used to enter user interface. The default code is 3888.

Press “*2396#” to enter administrator interface. Press “2” and “3” to enter service code setting interface to input a 4-digit new user code, and press “Dial key” to save.

3.3.3.Web Password Modify on Website

Login to the website and go to **Security** - **Basic**, to modify web password.

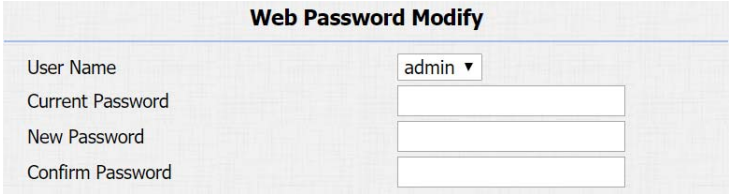

Figure 3.3.3 Web Password Modify

3.4.Phone Configuration

3.4.1.Language

Go to **Phone** - **Time/Lang** to select language for webpage.

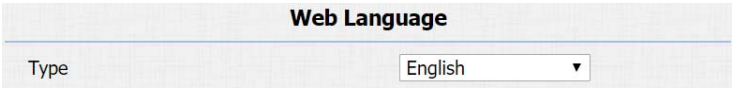

Figure 3.4.1 Language

3.4.2.Time

Go to **Phone** - **Time/Lang** to configure the time related features.

Format Setting: To select time format and date format.

Type: To select configure the time manually or automatically.

NTP: To select local time zone for NTP server.

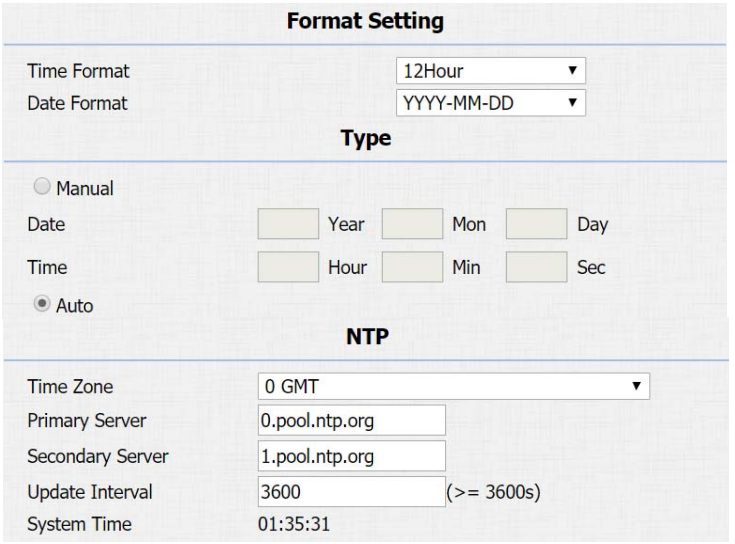

Figure 3.4.2 Time

3.4.3.Network

3.4.3.1.DHCP Mode

At device side, press “*2396#” to enter administrator interface. Press “3” to enter system setting interface, and press “1” to enter network setting interface.

Select DHCP mode, and R28 will access network automatically.

In website, go to **Network** - **Basic**.

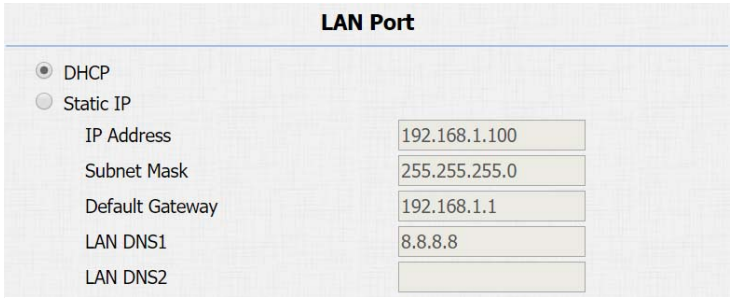

Figure 3.4.3.1 DHCP mode

R28 uses DHCP mode by default which will get IP address, subnet mask, default gateway and DNS server address from DHCP server automatically.

3.4.3.2.Static IP Mode

At device side, press “*2396#” to enter administrator interface. Press “3” to enter system setting interface, and press “1” to enter network setting interface.

Select static IP mode, users need to setup IP address, subnet mask, default gateway and DNS server address. Press “Dial key” when finish each step.

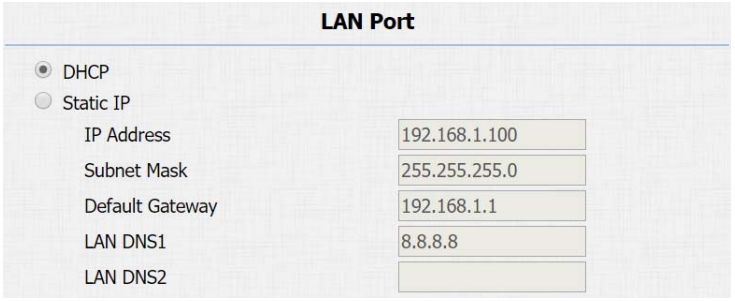

Figure 3.4.3.2 Static IP mode

In Website, go to **Network** - **Basic**.

If select static IP, users should manually setup IP address, subnet mask, default gateway and DNS server address. The figure right shows static IP settings.

3.4.3.3.Local RTP

Go to **Network** - **Advanced** to configure.

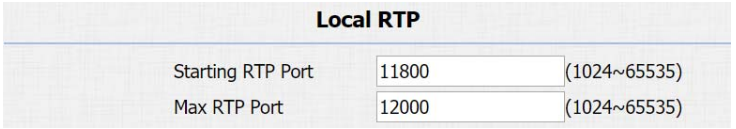

Figure 3.4.3.3 Local RTP

Local RTP: To display and configure local RTP settings.

Starting RTP Port: Determine the minimum port that RTP stream can use.

Max RTP Port: Determine the maximum port that RTP stream can use.

3.4.3.4.SNMP

Go to **Network** - **Advanced** to configure.

SNMP: To display and configure SNMP settings.

Active: To enable or disable SNMP feature.

Port: To configure SNMP server's port.

Trusted IP: To configure allowed SNMP server address. It could be an IP address or any valid URL domain name.

Note: SNMP is Internet-standard protocol for managing devices on IP networks.

Figure 3.4.3.4 SNMP

3.4.3.5.VLAN

Go to **Network** - **Advanced** to configure.

VLAN: To display and configure VLAN settings.

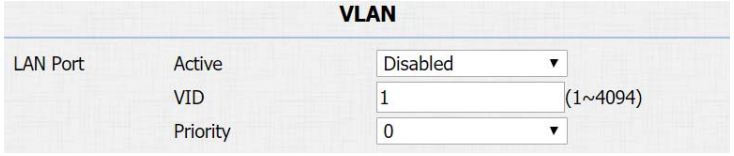

Figure 3.4.3.5 VLAN

Active: To enable or disable VLAN feature for designated port.

VID: To configure VLAN ID for designated port.

Priority: To select VLAN priority for designated port.

Note: Please consult administrator for specific VLAN settings in the networking environment.

3.4.3.6.TR069

Go to **Network** - **Advanced** to configure.

TR069: To display and configure TR069 settings.

Active: To enable or disable TR069 feature.

Version: To select supported TR069 version (version 1.0 or 1.1).

ACS/CPE: ACS is short for auto configuration servers as server side, and CPE is short for customer-premise equipment as client side devices.

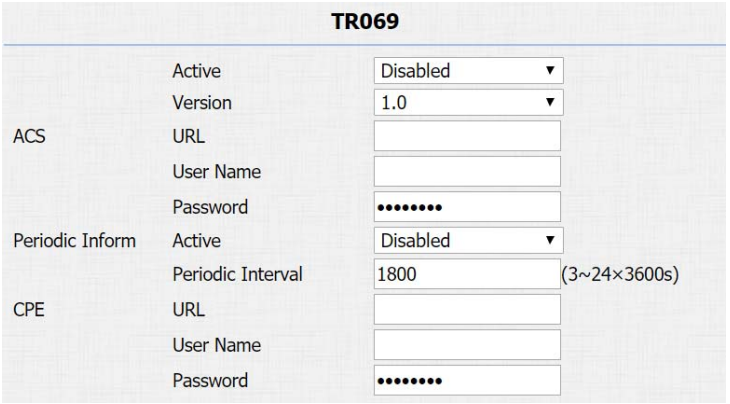

Figure 3.4.3.6 TR069

URL: To configure URL address for ACS or CPE.

User Name: To configure username for ACS or CPE.

Password: To configure password for ACS or CPE.

Periodic Inform: To enable periodically inform.

Periodic Interval: To configure interval for periodic inform.

Note: TR-069 is a technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices.

3.4.4.Display

Go to **Intercom** - **Basic** to configure display related features.

Display Number: To enable to display the number in LCD or not. If disabled, each number will be displayed as a star.

Figure 3.4.4-1 Display number

Go to **Intercom** - **Advanced** to configure display related features.

LCD Text: Users can customize the LCD text during the idle by themselves, such as “Welcome” or something else.

Figure 3.4.4-2 LCD display

AccountStatus Enabled: The LCD text will only be shown if the

the account is valid.

LCD Text Enable: Switch this feature.

LCD Text: Display content.

3.4.5.Voice

Login to the website and go to **Phone** - **Voice**, to configure voice parameters.

Go to **Phone** - **Voice** to configure volume and upload tone file.

Mic Volume: To configure microphone volume.

Speaker Volume: To configure speaker volume.

Open Door Warning: Disable it, and users will not hear the prompt voice when the door is opened.

RingBack Upload: To upload the ring back tone by users themselves.

Opendoor Tone Upload: To upload the open door tone by users themselves.

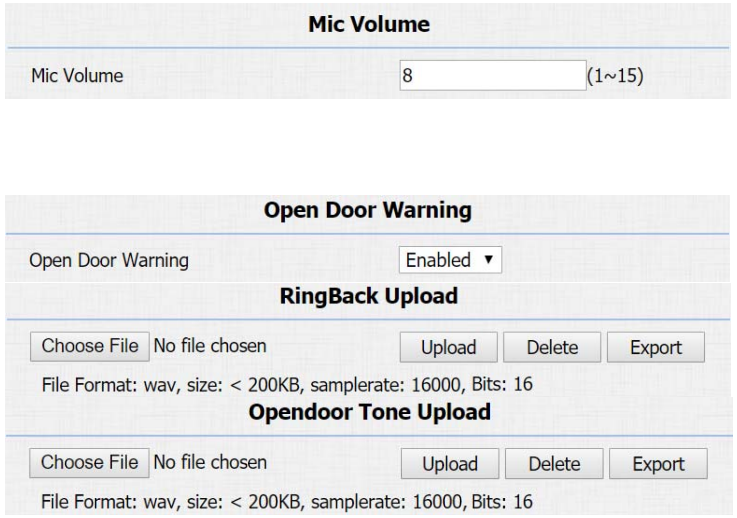

Figure 3.4.5 Voice

3.5.Intercom Call

3.5.1.Direct IP Call

Go to **Phone** - **Call Feature** to enable the direct IP call for door phones first.

In the idle interface, press the IP address (like IP address 192.168.1.100, users need to press “192*168*1*100”) and “Dial key” to make a direct IP call.

Figure 3.5.1 Direct IP call

3.5.2.SIP Call

SIP calls which use SIP numbers to make or receive calls should be supported by SIP server. Users need to register accounts and fill SIP feature parameters before using it.

Go to **Account** - **Basic** to configure SIP account and SIP server for door phones first.

3.5.3.SIP Account

Status: To display register result.

Display Label: To configure label displayed on the phone’s

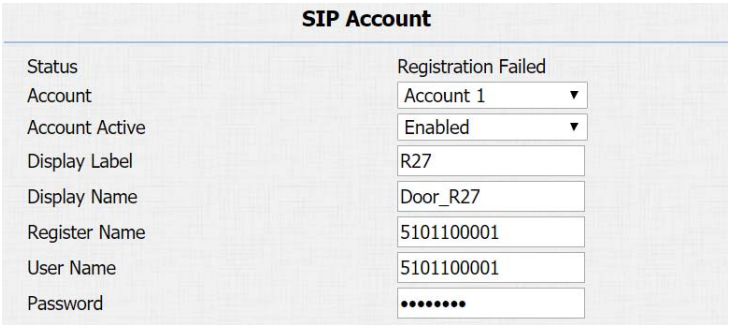

Figure 3.5.3 SIP account

LCD screen.

Display Name: To configure name sent to the other call party for displaying.

Register Name: To enter extension number which users want and the number is allocated by SIP server.

User Name: To enter user name of the extension.

Password: To enter password for the extension.

3.5.4.SIP Server 1&2

Server IP 1: To enter SIP server's IP address or URL.

Server IP 2: To display and configure secondary SIP server settings. This is for redundancy, if registering to primary SIP server fails, the phone will go to secondary SIP server for registering.

Registration Period: The registration will expire after registration period, and the phone will re-register automatically within registration period.

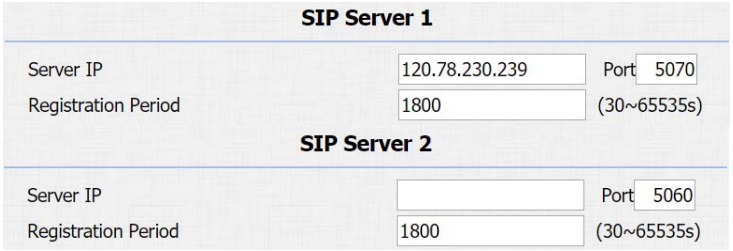

Figure 3.5.4 SIP server 1&2

3.5.5.Outbound Proxy Server

An outbound proxy server is used to receive all initiating request messages and route them to the designated SIP server.

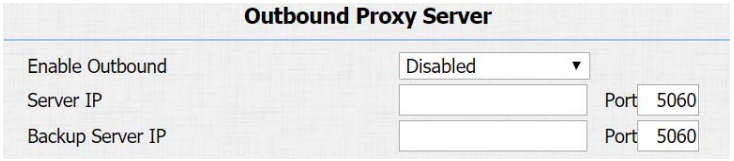

Figure 3.5.5 Outbound proxy server

3.5.6.Transport Type

To display and configure transport type for SIP message.

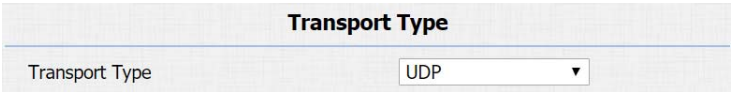

Figure 3.5.6 Transport type

- UDP: UDP is an unreliable but very efficient transport layer protocol.
- TCP: Reliable but less-efficient transport layer protocol.
- TLS: Secured and reliable transport layer protocol.
- DNS-SRV: DNS record for specifying the location of services.

3.5.7.NAT

To display and configure NAT settings.

Figure 3.5.7 NAT

- STUN: Short for session traversal utilities for NAT, a solution to solve NAT issues.

Note: By default, NAT is disabled.

In the idle interface, press the a SIP account and “Dial key” to make a SIP call.

3.5.8.Dial Plan

This feature allows users to modify selected rules information.

Once users dial prefix value, it will call out replace number.

Go to **Intercom** - **Basic** to configure first.

Rules Management

R28 supports to import or export the dial plan rules, which is convenient for administrator to deal with a large number of dial plan. The maximum dial plan is 200.

Note: Please consult administrator for the .xml format dial plan template file.

Edit Dial plan

- Click “Add” to add new replace rules.
- Select account for the replace rule.
- Enter a display name for the prefix value. Input a suitable

Figure 3.5.8-1 Dial plan rules management

Figure 3.5.8-2 Dial plan rules

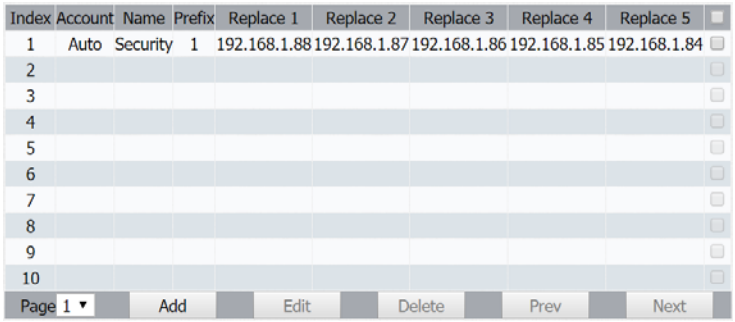

Figure 3.5.8-3 Dial plan

prefix value. Enter the replace number.

- Click “Submit” to save.

All replace rules will show in the list. Users can edit or delete the existed replace rules.

In the idle interface, press the prefix and “Dial key” to make a call.

3.5.9.Speed Dial

Speed dial feature is used to call out 4 numbers at the same time.

Go to **Intercom** - **Basic** to configure first.

After setup the number which users need to call, in the idle interface, press “Manage center key” (Manager Dial) or “Dial key” (Speed Dial) to call.

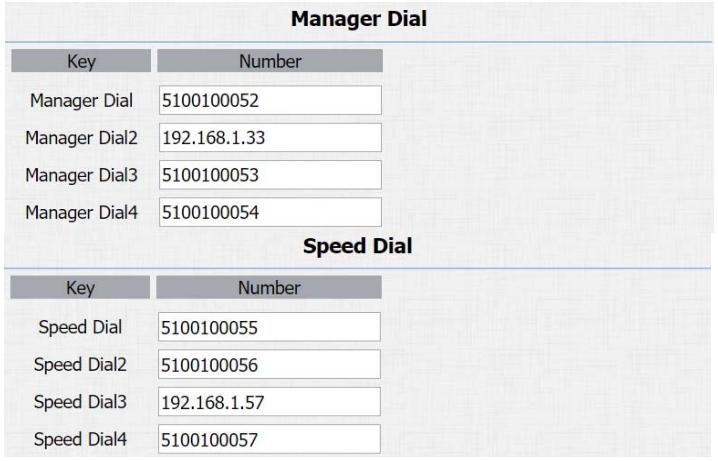

Figure 3.5.9 Speed dial

3.5.10.Auto Answer

Go to **Account** - **Advanced** to enable auto answer feature for SIP calls.

Figure 3.5.10-1 Auto answer for sip calls

Figure 3.5.10-2 Auto answer for direct IP calls

Go to **Phone** - **Call Feature** to enable auto answer feature for direct IP calls.

Auto Answer Delay: To configure delay time before an incoming call is automatically answered.

Auto Answer Mode: To set video or audio mode for auto answer feature. It is video by default.

Then incoming calls will be answered automatically.

Figure 3.5.10-3 Auto answer options' parameters

3.5.11Web Call

Go to **Intercom** - **Basic** to dial out or hang up incoming calls

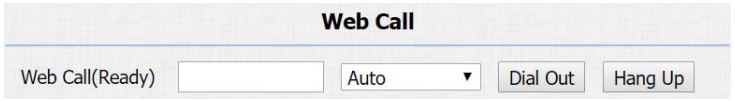

Figure 3.5.11 Web call

3.5.12.Multicast

Go to **Intercom** - **Multicast** to configure.

Paging Barge: Choose the multicast number, and the range is from 1 to 10.

Paging priority Active: Enable or disable the multicast.

Listening Address: Enter IP address which users need to listen.

Label: Input the label for each listening address.

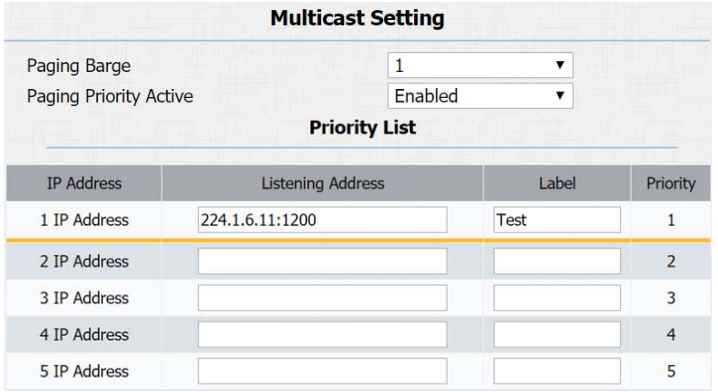

Figure 3.5.12 Multicast

3.6.Security

3.6.1.Live view

Go to **Intercom** - **Live Stream** to check the real-time video from R28.

Figure 3.6.1 Live view

3.6.2.RTSP

R28 supports RTSP stream, go to **Intercom** - **RTSP** to enable or disable RTSP server. The URL for RTSP stream is: **rtsp://IP_address/live/ch00_0**.

RTSP Stream: To enable RTSP video and select the video codec. R28 supports H.264 video codec by default.

H.264 Video Parameters: H.264 is a video stream compression standard. Different from H.263, it provides an approximately identical level of video stream quality but a half bit rate. This type of compression is sometimes called MPEG-4 part 10. To modify the resolution, framerate and bitrate of H.264.

MPEG4 Video Parameters: MPEG4 is one of the network video

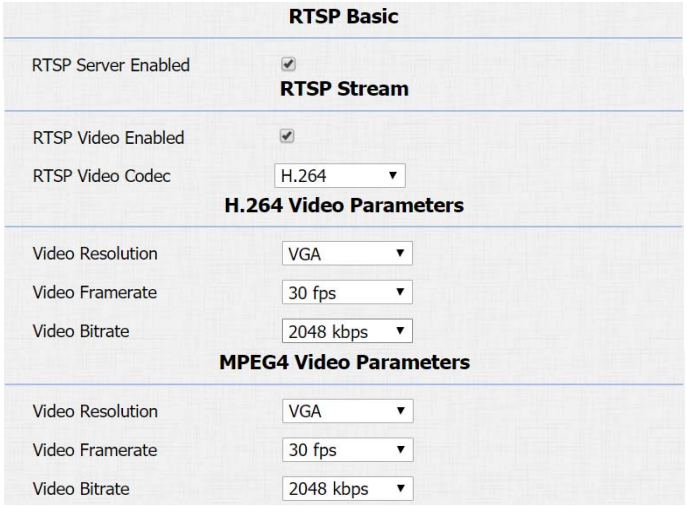

Figure 3.6.2 RTSP

image compression standard. It supports the maximum compression ratio 4000:1. It is an important and common video function with great communication application integration ability and less core program space. To modify the resolution, framerate and bitrate of MPEG4.

3.6.3.ONVIF

R28 supports ONVIF protocol, which means R28's camera can be searched by other devices, like NVR which supports ONVIF protocol as well.

Go to **Intercom** - **ONVIF** to configure ONVIF mode, its username and password.

Switching ONVIF mode to "Undiscoverable," and it means users must program ONVIF's URL manually.

The ONVIF's URL is:

http://IP_address:8090/onvif/device_service.

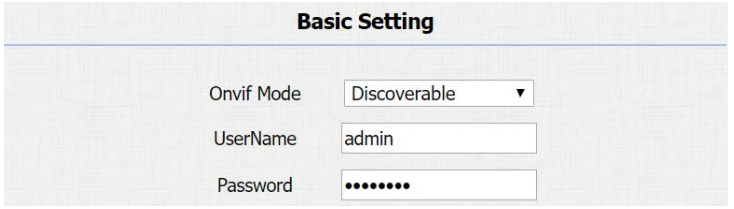

Figure 3.6.3 ONVIF

3.7.Access Control

Login to the website and go to Phone - Time/Lang, to configure time and language

3.7.1.Relay

Go to **Intercom** - **Relay** to configure relay settings.

There are three terminals of relay: NO, NC and COM. NO stands for normally open contact. NC stands for normally closed contact.

Relay ID: R28 supports three relays. Users can configure them respectively.

Relay Type: Default state means NC and COM are normally closed, while Invert state means NC and COM are normally opened.

Relay Delay: To configure the duration of opened relay. Over the value, the relay would be closed again.

Relay Status: While the relay is triggered, the statues will be switched. When COM connects to NC, the status is low.

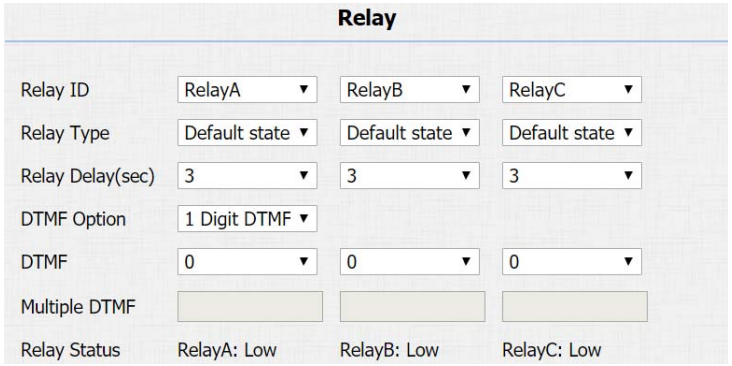

Figure 3.7.1 Relay

Note: Relay does not deliver power. users should prepare power adapter for external devices which connects to relay.

3.7.2.DTMF Code

Users can unlock via a DTMF code when in a call.

Go to **Intercom** - **Relay** to configure DTMF code parameters.

DTMF Option: To select digit of DTMF code.

DTMF&Multiple DTMF: To configure DTMF code for remote unlocking.

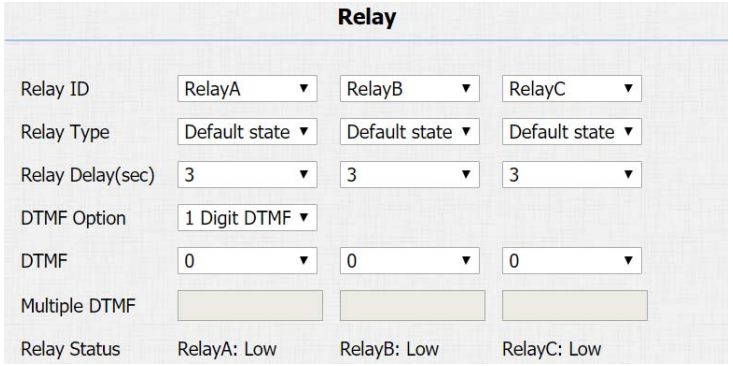

Figure 3.7.2 DTMF Code

3.7.3.HTTP Command

Users can use a URL to remote unlock the door.

Go to **Intercom** - **Relay** to configure.

Switch: Enable this function. Disable by default.

UserName&Password: Users can setup the username and password for HTTP unlock.

URL format:

http://IP_address/fcgi/do?action=OpenDoor&UserName=&Password=&DoorNum=1.

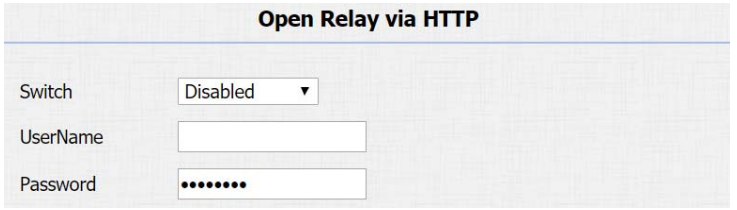

Figure 3.7.3 HTTP Command

3.7.4.RF Card

Go to **Intercom** - **Card setting** to manage card access system.

1.Import/Export Card Data

R28 supports import or export card data, which is convenient for administrator to deal with a large number of cards.

The maximum card data file is 200K which is around 500 cards.

2.Obtain and Add Card

- Switch card status to “Card Issuing” and click “Apply”;
- Place card on the card reader area and click “Obtain”;
- Name card, choose which door users want to open and the valid day and time;
- Click “Add” to add it into list.

Valid card information will be shown in the list. Administrator could delete one card’s access permission or empty all the list.

Note: Remember to set Card Status back to “Normal” after adding cards.

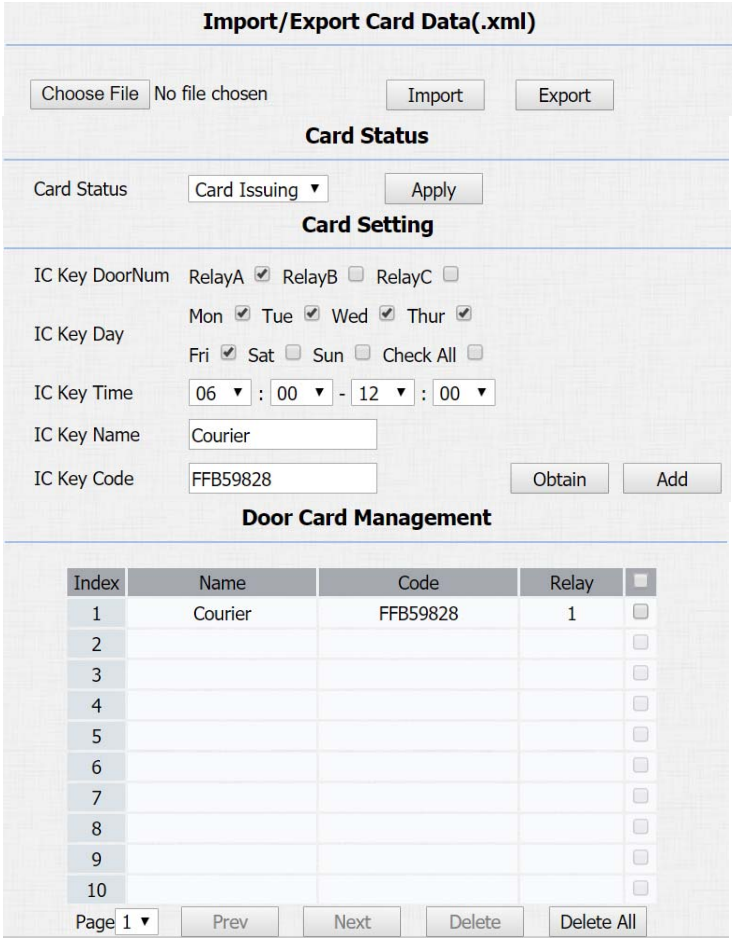

Figure 3.7.4 RF cards

3.7.5.Public Key

Go to Intercom - Basic - Public Key, to setup public key for PIN Entry

Key Switch: Enable or Disable the public key.

Key Value: Type in a PIN code as public key.

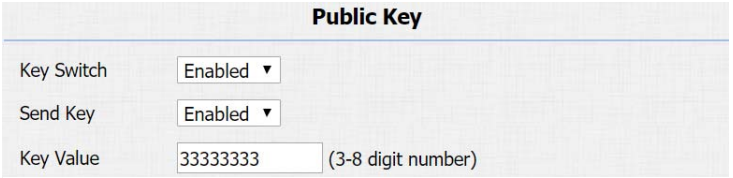

Figure 3.7.5 Public Key

3.7.6.Private Key

Go to **Intercom** - **PrivateKey** to configure private pin code.

Import /Export Private Key

R28 supports import or export the private key file, which is convenient for administrator to deal with a large number of private keys.

The maximum private key is 500.

Note: Please consult administrator for the .xml format private key template file.

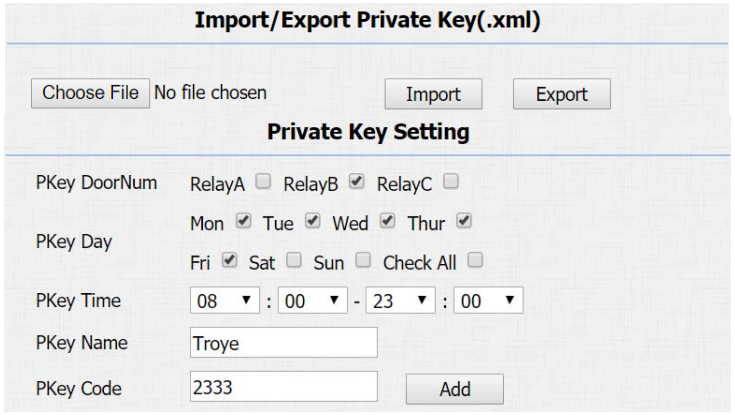

Figure 3.7.6 Private Key

Obtain and Add Private Key

- Enter the “PKey Name” and 3-8 digits “PKey Code”;
- Select the valid day and time;

- Choose which door users want to open;
- Click “Add” to add it into list.

Valid private key information will be shown in the list. Administrator could delete private key information or empty all the list.

3.7.7.Input

R28 supports three input triggers “Input A/B/C(DOOR A/B/C).

Go to **Intercom** - **Input** to configure input settings.

Input Service: To enable or disable input trigger service.

Trigger Option: To choose open circuit trigger or closed circuit trigger. “Low” means that connection between door terminal and GND is closed, while “High” means the connection is opened.

Door status: To show the status of input signal.

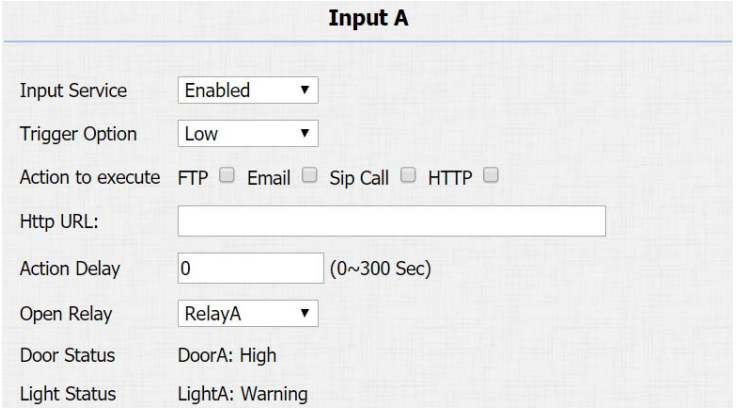

Figure 3.7.7 Input

3.8.Reboot

Go to **Upgrade** - **Basic**, users can reboot the phone.

Figure 3.8 Reboot

3.9.Restore

3.9.1.Restore Default on R28

Go to **Settings** - **System Settings** - **Restore Default** on R28, to restore R28.

3.9.2.Reset To Factory Setting on Website

Login to the website and go to **Upgrade - Basic**, to restore R28.

Figure 3.9.2 Reset in website

4.Advanced Features

4.1Advanced Display

4.1.1LED

Go to **Intercom** - **LED Setting** to configure.

Users can control three parts' LED, screen, keypad and card area. Users can also setup the valid time. For example, start time from 18 to 23 means the LED will light up from 6pm to 11pm.

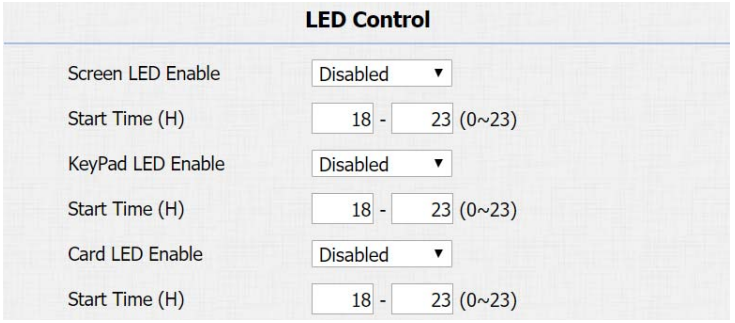

Figure 4.1.1 LED

4.1.2.IR LED

Go to **Intercom** - **Advanced** to configure.

Photoresistor: The setting is for night vision, when the surrounding of R28 is very dark, infrared LED will turn on and R28 will turn to night mode.

Photoresistor value relates to light intensity and larger value means that light intensity is smaller.

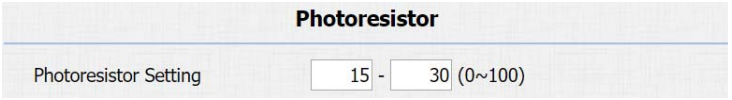

Figure 4.1.2 IR LED

Users can configure the upper and lower bound and when photoresistor value is larger than upper bound, infrared LED will turn on. As contrast, when photoresistor value is smaller than lower bound, infrared LED will turn off and device turns to normal mode.

4.1.3.RFID Card Code Display Related

Go to **Intercom** - **Advanced** to configure.

Display mode: To be compatible different card number formats in different systems. The default 8HN means hexadecimal.

Figure 4.1.3 RFID card code display related

4.1.4.Key Display Related

Go to **Intercom** - **Basic** to configure.

Send Key: Limit to use the “#” key. It will prevent someone to enter the LCD setting illegally.

Figure 4.1.4-1 Send key

DialPad Input Number Limit: To limit the input numbers to prevent unnecessary security problems.

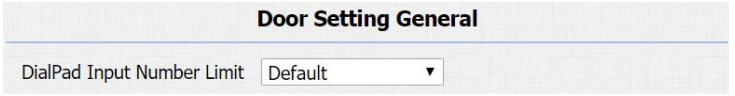

Figure 4.1.4-2 Dialpad input number limit

4.2.Intercom

4.2.1.Max Call Time

Go to **Intercom** - **Basic** to configure Max Cenne shia all time.

Dial In Time: To configure the max incoming dial time, available when auto answer is disabled.

Dial Out Time: To configure the max no answer call time.

Figure 4.2.1 Call time related

4.2.2.AEC Level

Go to **Intercom** - **Basic** to configure AEC Setting

AEC Level: AEC is used to adjust the echo effect during the communication. The default value is 700. Increase the level, the echo control is better.

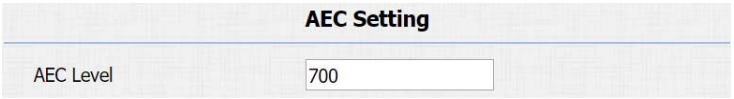

Figure 4.2.2 AEC level

4.2.3.Intercom

Go to **Phone** - **Call Feature** to configure.

Intercom: Intercom allows users to establish a call directly with the callee.

Active: To enable or disable Intercom feature.

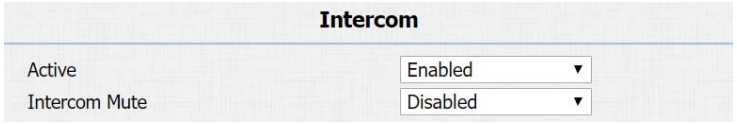

Figure 4.2.3 Intercom

Intercom Mute: If enabled, once the call established, the callee will be muted.

4.2.4.Return Code When Refuse

Go to **Phone** - **Call Feature** to configure.

Return Code When Refuse: Allows users to assign specific code as return code to SIP server when an incoming call is rejected.

Figure 4.2.4 Return code when refuse

4.2.5.SIP Call Related

Go to **Account** - **Advanced** to configure the SIP call related.

Max Local SIP Port: To configure maximum local SIP port for designated SIP account.

Min Local SIP Port: To configure maximum local SIP port for designated SIP account.

Caller ID Header: To choose caller ID header format.

Provisional Response ACK: 100% reliability for all provisional messages, this means it will send ACK every time the phone receives a provisional SIP message from SIP server.

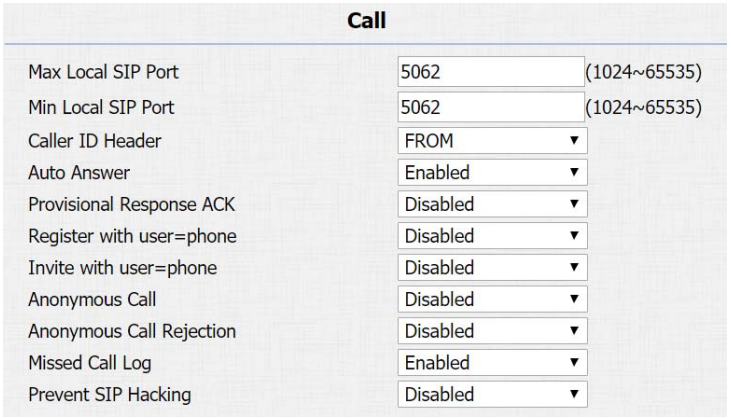

Figure 4.2.5 SIP call related

Register with user=phone: If enabled, the phone will send user=phone within SIP message.

Anonymous Call: If enabled, R28 will block its information when calling out.

Anonymous Call Rejection: If enabled, calls who block their information will be screened out.

Missed Call Log: If enabled, any missed call will be recorded into call log.

Prevent Hacking: If enabled, it will prevent SIP messages from hacking.

4.2.6.Codec

Go to **Account** - **Advanced** to configure SIP call related codec.

Sip Account: To choose which account to configure.

Audio Codec: R28 support four audio codecs: PCMA, PCMU, G729, G722. Different audio codecs require different bandwidth, users can enable/disable them according to different network environment.

Note: Bandwidth consumption and sample rates are as below:

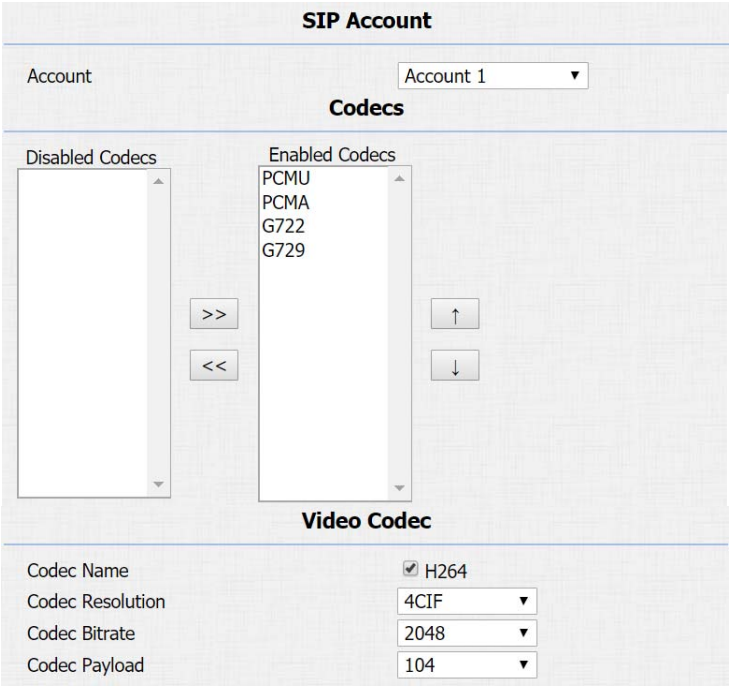

Figure 4.2.6-1 SIP call related codec

Codec	Bandwidth	Sample Rates
PCMA	64kbit/s	8kHz
PCMU	64kbit/s	8kHz
G729	8kbit/s	8kHz
G722	64kbit/s	16kHz

Video Codec: R28 support H.264 standard, which provides better video quality at substantially lower bit rates than previous standards.

Codec Resolution: R28 support four resolutions, QCIF, CIF, VGA, 4CIF and 720P.

Codec Bitrate: To configure bit rates of video stream.

Codec Payload: To configure RTP audio video profile.

Go to **Phone** - **Call Feature** to configure multicast related codec.

Figure 4.2.6-2 Multicast related codec

4.2.7.Subscribe

Go to **Account** - **Advanced** to configure.

MWI: Message waiting indicator which is used to indicate whether there is unread new voice message.

BLF: BLF is short for busy lamp field which is used to monitor the designated extension status.

ACD: Automatic call distribution is often used in offices for customer service, such as call center. The setting here is to negotiate with the server about expire time of ACD subscription.

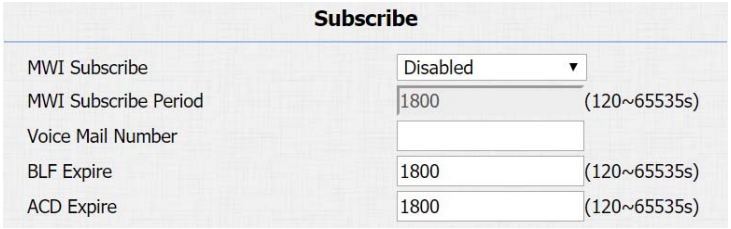

Figure 4.2.7 Subscribe

4.2.8.DTMF

Go to **Account** - **Advanced** to configure RTP audio video profile for DTMF and its payload type.

Type: Support inband, info, RFC2833 or their combination.

How To Notify DTMF: Only available when DTMF type is info.

DTMF Payload: To configure payload type for DTMF.

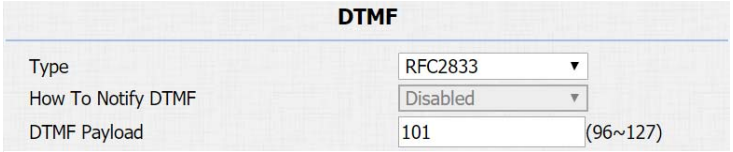

Figure 4.2.8 DTMF

4.2.9.Session Timer

Go to **Account** - **Advanced** to configure.

If enabled, the on going call will be disconnected automatically once the session expired unless it's been refreshed by UAC or UAS.

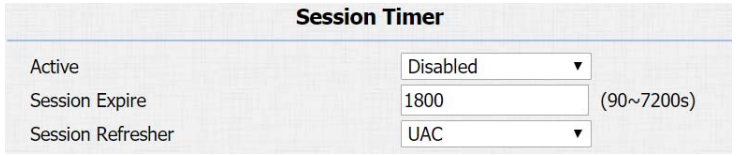

Figure 4.2.9 Session timer

4.2.10.Encryption

Go to **Account** - **Advanced** to configure.

If enabled, voice will be encrypted.

Figure 4.2.10 Encryption

4.2.11.NAT

Go to **Account** - **Advanced** to display NAT related settings.

UDP Keep Alive message: If enabled, the phone will send UDP keep-alive message periodically to router to keep NAT port alive.

UDP Alive Msg Interval: Keep alive message interval.

Rport: Remote port, if enabled, it will add remote port into outgoing SIP message for designated account.

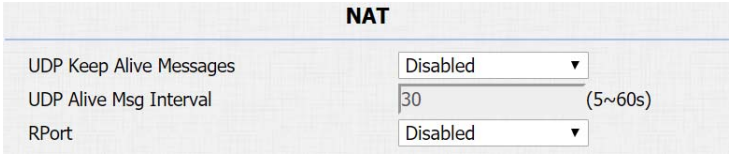

Figure 4.2.11 NAT

4.2.12.User Agent

Go to **Account** - **Advanced** to configure. One can customize user agent field in the SIP message. If user agent is set to specific value, users can see the information from PCAP. If user agent is not set by default, users can see the company name, model number and firmware version from PCAP.

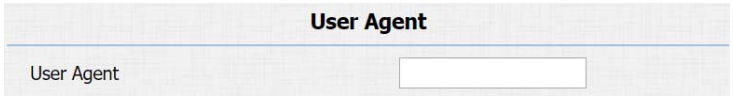

Figure 4.2.12 User Agent

4.3.Access Control

4.3.1.Web Relay

R28 can support to connect to web relay.

Go to **Phone** - **WebRelay** to configure.

Type: Connect web relay and choose the type.

IP Address: Enter web relay's IP address.

User Name: it is an authentication for connecting web relay.

Password: It is an authentication for connecting web relay.

Web Relay Action: Web relay action is used to trigger the web relay. The action URL is provided by web relay vendor.

Figure 4.3.1-1 Web relay

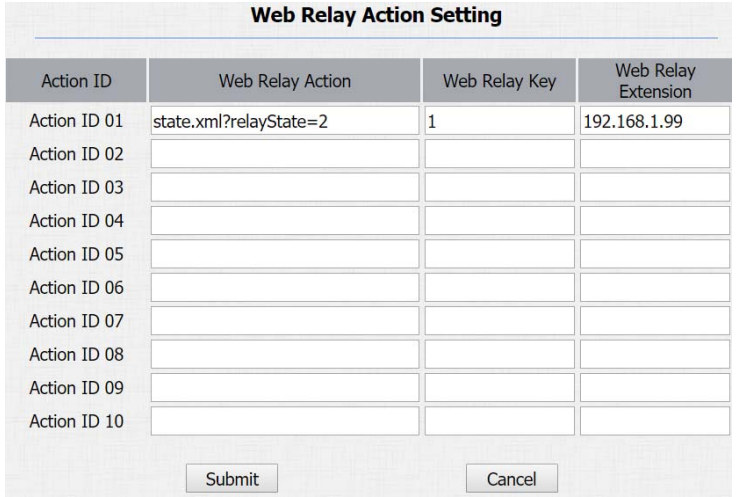

Figure 4.3.1-2 Web relay action settings

Web Relay Key: If the DTMF keys are same with the local relay, the web relay will be open with local relay. But if there are different, the web relay is invalid.

Web Relay Extension: The web relay can only receive the DTMF signal from the corresponding extension number.

Note: Users can modify username and password in web relay website.

4.3.2.Wiegand

Using this feature to integrate with some wiegand access control. R28 can be used as wiegand input or output.

Go to **Intercom** - **Advanced** to configure.

Wiegand Type: Support Wiegand 26 or 34. The different number means different bits.

Wiegand Mode: Input or output. Typically, when users select input, we generally connect the wiegand input device, such as the wiegand card reader. Or R28 can be used as output, it is generally used to connect the third-party access control, and R28 change the card information as wiegand signal, and then

Figure 4.3.2 Wiegand

transfer to the access control module.

4.4.Security

4.4.1.Anti-alarm

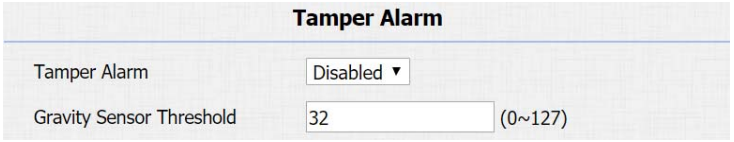

Figure 4.4.1 Anti-alarm

Go to **Intercom** - **Advanced** to configure.

Tamper Alarm: R28 integrates internal gravity sensor for its own security. After enabling tamper alarm, if the gravity of R28 changes dramatically, it will alarm. Gravity sensor threshold stands for sensitivity of sensor. Smaller the value, the more sensitive it is.

4.4.2.Motion

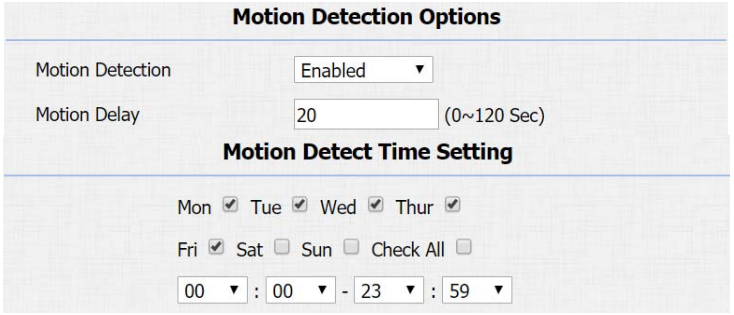

Figure 4.4.2 Motion

R28 supports motion detection, go to **Intercom** - **Motion** to configure detection related parameters.

Motion Detection: To enable or disable motion detection.

Motion Delay: To configure minimum time gap between two snapshots.

Motion Detect Time Setting: To configure motion detect time

schedule.

4.5.Action

R28 supports to send notifications, snapshots via email and ftp transfer method, or calls via sip call method, when trigger specific actions.

4.5.1.Action Parameters

Go to **Intercom** - **Action** to set action receiver.

Email Notification

Sender's email address: To configure email address of sender.

Receiver's email address: To configure email address of receiver.

SMTP server address: To configure SMTP server address of sender.

SMTP user name: To configure user namer of SMTP service (usually it is same with sender's email address).

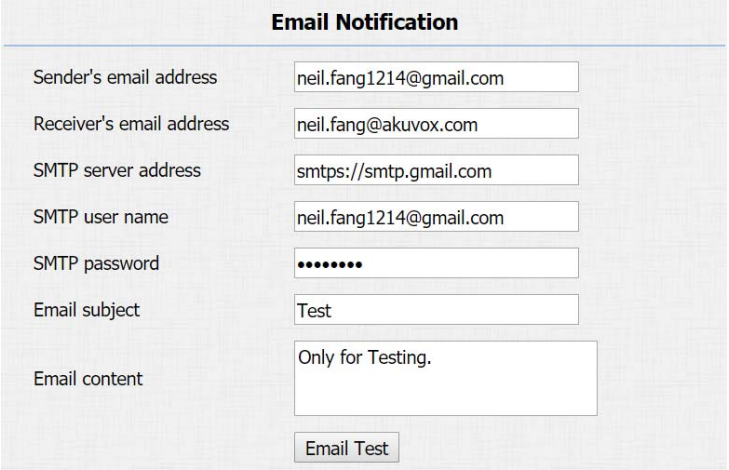

Figure 4.5.1 Email notification parameters

SMTP password: To configure password of SMTP service (usually it is the same with the password of sender's email).

Email subject: To configure subject of email.

Email content: To configure content of email.

Email Test: To test whether email notification is available.

FTP Notification

FTP Server: To configure URL of FTP server.

FTP User Name: To configure user name of FTP server.

FTP Password: To configure password of FTP server.

FTP Test: To test whether FTP notification is available.

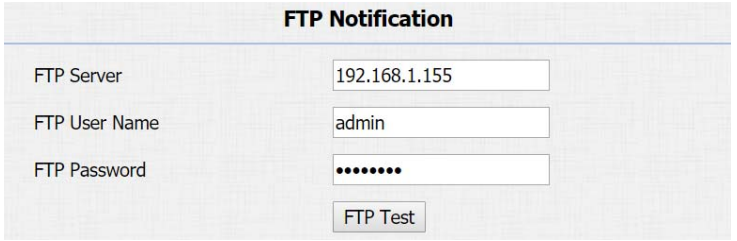

Figure 4.5.1-2 FTP notification parameters

SIP Notification

SIP Call Number: To configure sip call number.

SIP Call Name: To configure display name of R28.

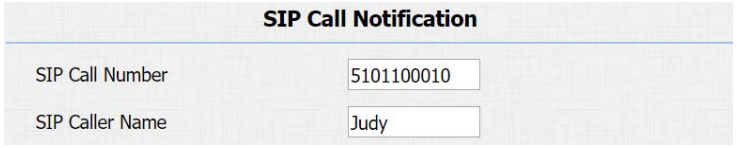

Figure 4.5.1-3 SIP call notification parameters

Five specific actions which will be triggered in R28:

4.5.2.No Answer Action

Go to **Intercom** - **Basic** to configure.

No Answer Action: For sending the notification to specified email if the call is not answered.

Figure 4.5.2 No answer action

4.5.3.Call Event

Go to **Intercom** - **Basic** to configure.

Action to execute: To choose suitable way to receive message or snapshot when dialing out.

HTTP URL: If users choose HTTP mode, enter the URL format: http://http server IP address/any information.

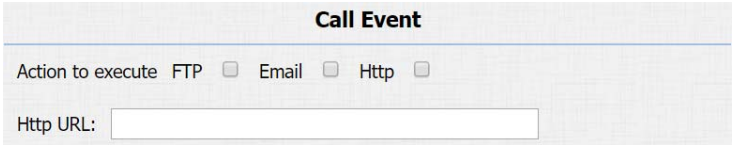

Figure 4.5.3 Call event

4.5.4.Input Interface Triggered Action

Go to **Intercom** - **Input** to configure.

Action to execute: To choose which action to execute after triggering.

Http URL: To configure URL, if HTTP action is chosen.

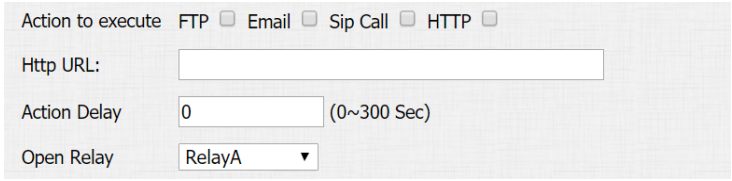

Figure 4.5.4 Input interface triggered action

Action Delay: To configure after how long to execute to send out notifications and trigger relay.

Open relay: To configure which relay to trigger.

4.5.5.Motion Triggered Action

Go to **Intercom** - **Motion** to configure.

Action to execute: To choose which action to execute after triggering.

Http URL: To configure URL, if HTTP action is chosen.

SDMC Upload: Upload the capture to the SDMC.

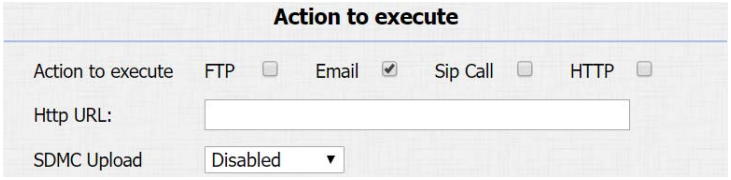

Figure 4.5.5 Motion triggered action

4.5.6.Unlock via RFID Card Action

Go to **Intercom** - **Card Setting** to configure.

Action to execute: To choose which action to execute after unlocking via a RFID card.

Http URL: To configure URL, if HTTP action is chosen.

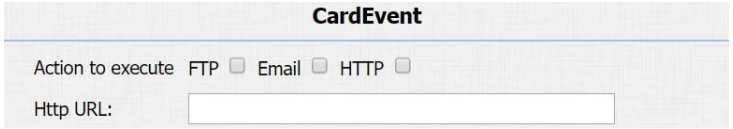

Figure 4.5.6 Unlock via RFID card action

4.6.Upgrade

4.6.1.Web Upgrade

Go to **Upgrade** - **Basic** to do web upgrade.

Upgrade: Choose .rom firmware from the PC, and then click "Submit" to start update.

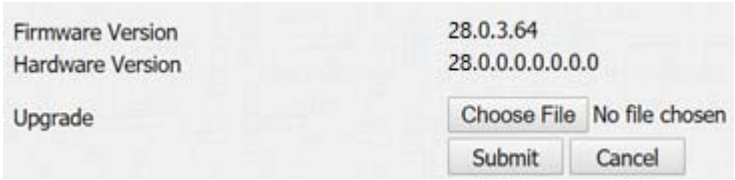

Figure 4.6.1 Web upgrade

4.6.2.Autop Upgrade

Go to **Upgrade** - **Advanced** to configure automatically update server's settings.

PNP

Plug and Play, once PNP is enabled, the phone will send SIP subscription message to PNP server automatically to get auto provisioning server's address.

By default, this SIP message is sent to multicast address 224.0.1.75 (PNP server address by standard).

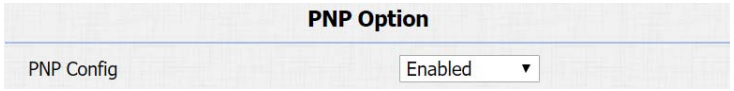

Figure 4.6.2-1 PNP

Manual Autop

Autop is a centralized and unified upgrade for phones. It is also a simple and time-saving configuration for phones. It is mainly used by devices to download corresponding configuration documents from the server which is using TFTP / FTP / HTTP / HTTPS network protocol. Achieving the purpose for updating devices's configurations and making users to change the phone configuration more easily, it is a typical C/S architecture upgrade mode, which is mainly used by the terminal device or PBX server to initiate an upgrade request.

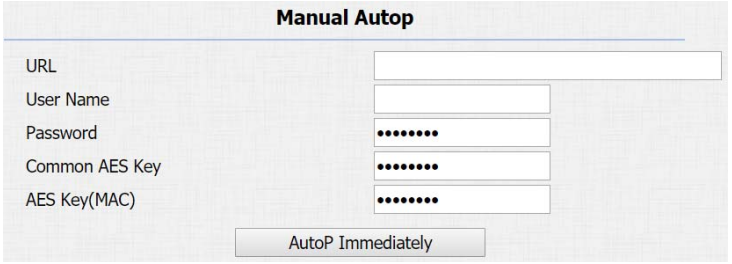

Figure 4.6.2-2 Manual auto provision

URL: Auto provisioning server address.

User Name: Configure if server needs an username to access, otherwise left blank.

Password: Configure if server needs a password to access, otherwise left blank.

Common AES Key: Used for the phone to decipher common auto provisioning configuration file.

AES Key (MAC): Used for the phone to decipher MAC-oriented auto provisioning configuration file (for example, file name could be 0c1105888888.cfg if phone's MAC address is 0c1105888888).

Note: AES should be configured only when configure file is ciphered with AES, otherwise left blank.

Automatic Autop

To display and configure auto provisioning mode settings.

This auto provisioning mode is actually self-explanatory.

For example, mode "Power on" means the phone will go to do provisioning every time it powers on.

Note: Please refer to the related feature guide from forum.

4.6.3.Backup Config File

Go to **Upgrade** - **Advanced** to backup the config file.

Export Autop Template: To export current config file.

Others: To export current config file (Encrypted) or import new config file.

Figure 4.6.3-1 Backup config file

4.7.Log

4.7.1.Call Log

Go to **Phone** - **Call Log**, users can see a list of call logs which have dialed, received or missed. Users can delete call logs from list.

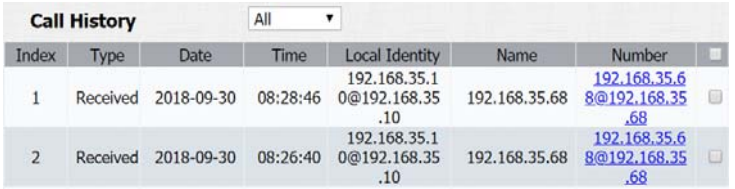

Figure 4.7.1 Call log

4.7.2.Door Log

Go to **Phone** - **Door Log**, users can see a list of door logs which records card information and date.

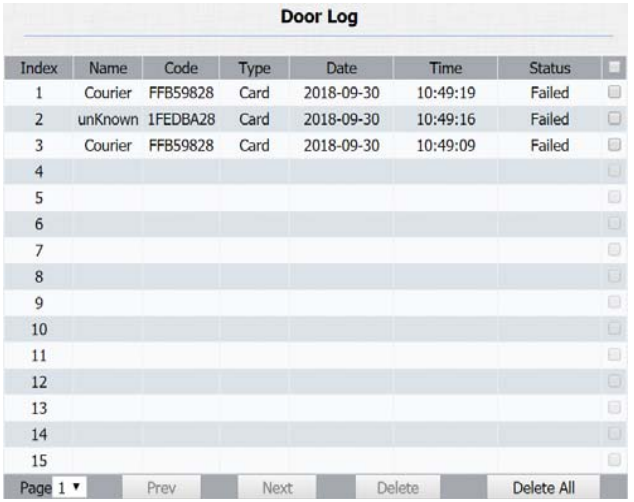

Figure 4.7.2 Door log

4.7.3.System Log

Go to **Upgrade** - **Advanced** to configure system log level and export system log file.

System log level: From level 0 to 7. The higher level means the more specific system log is saved to a temporary file. It's level 3 by default.

Export Log: Click to export temporary system log file to local PC.

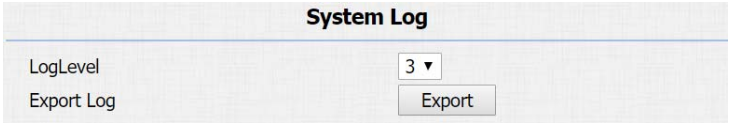

Figure 4.7.3 System log

4.7.4.PCAP

Go to **Upgrade** - **Advanced** to start, stop packets capturing or to export captured packet file.

Start: To start capturing all the packets file sent or received from phone.

Stop: To stop capturing packets.

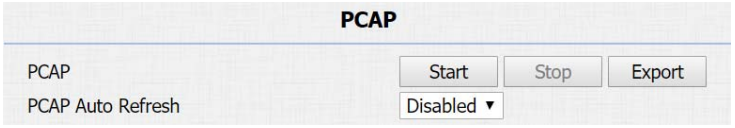

Figure 4.7.4 PCAP

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

IP: Internet Protocol

ID: Identification

IR: Infrared

LCD: Liquid Crystal Display

LED: Light Emitting Diode

MAX: Maximum

POE: Power Over Ethernet

PCMA: Pulse Code Modulation A-Law

PCMU: Pulse Code Modulation μ-Law

PCAP: Packet Capture

PNP: Plug and Play

RFID: Radio Frequency Identification

RTP: Real-time Transport Protocol

RTSP: Real Time Streaming Protocol

MPEG: Moving Picture Experts Group

MWI: Message Waiting Indicator

NO: Normal Opened

NC: Normal Connected

NTP: Network Time Protocol

NAT: Network Address Translation

NVR: Network Video Recorder

ONVIF: Open Network Video Interface Forum

SIP: Session Initiation Protocol

SNMP: Simple Network Management Protocol

STUN: Session Traversal Utilities for NAT

SNMP: 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

Contact us

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

Sales email: sales@akuvox.com

Technical support email: techsupport@akuvox.com

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

We highly appreciate your feedback about our products.