RTSP Stream Monitoring

You can use RTSP to watch a live video stream from other intercom devices on the device.

RTSP Basic Setting

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

RTSP Basic

Enabled	☑
RTSP Authorization Enabled	☐
MJPEG Authorization Enabled	☑
Authentication Mode	Digest ▼
User Name	admin
Password	••••••

- **RTSP Authorization Enabled**: Once enabled, configure RTSP Authentication Mode, RTSP Username, and RTSP Password. These credentials are required for accessing the door phone's RTSP stream from other intercom devices like indoor monitors.
- **Authentication Mode**: Select between Basic and Digest. It is Digest by default that uses hashing instead of the easily reversible Base64 encoding. A token is used for verification.
- **User Name**: Set the username for authorization.
- **Password**: Set the password for authorization.

RTSP Stream Setting

The RTSP stream can use H.264 as the video codec. You can adjust the video resolution, bitrate, and other settings on the web **Surveillance > RTSP > H.264 Video Parameters** interface.

H.264 Video Parameters

Main Video 1 Resolution	4CIF
Main Video 1 Framerate	30fps
Main Video 1 Crop Mode	Original
Main Video 1 Bitrate	2048kbps
Main Video 2 Resolution	720P
Main Video 2 Framerate	30fps
Main Video 2 Crop Mode	Crop
Main Video 2 Bitrate	2048kbps
Auxiliary Video 1 Resolution	720P
Auxiliary Video 1 Framerate	30fps
Auxiliary Video 1 Bitrate	2048kbps

- **Main Video 1 Resolution**: Specify the image resolution for the first video stream channel of the main camera, varying from the lowest QCIF(176×144 pixels) to the highest 2K(2560×1440 pixels). The default is 4CIF.
- **Main Video 2 Resolution**: Specify the image resolution for the second video stream channel of the main camera, varying from the lowest QCIF(176×144 pixels) to the highest 1080P(1920x1080 pixels). The default is 720P.
- **Main Video 1/2 Framerate**: Frames per second refers to how many frames are displayed in one second of video. The default frame rate is 30fps.
- **Main Video 1/2 Crop Mode**:
    - **Crop**: The transmitted video frame is cropped to eliminate vignettes.
    - **Original**: The original video frame is transmitted without cropping.
- **Main Video Video 1/2 Bitrate**: The amount of video data transferred in a specific duration of time. A higher video bitrate means a higher possible quality, but also higher file sizes and more bandwidth. The default is 2048 kbps.
- **Auxiliary Video 1 Resolution**: Specify the image resolution for the first and second video stream channels of the auxiliary camera at the bottom of the device, varying from the lowest QCIF(176×144 pixels) to the highest 1080P(1920x1080 pixels). The default is 720P.

- **Auxiliary Video 1 Framerate**: Frames per second refers to how many frames are displayed in one second of video. The default frame rate is 30fps.
- **Auxiliary Video 1 Bitrate**: The amount of video data transferred in a specific duration of time. A higher video bitrate means a higher possible quality, but also higher file sizes and more bandwidth. The default is 2048 kbps.

> **Tip**
>
> To view the audio and video stream using RTSP:
>
> - First channel: rtsp://Device's IP/live/ch00_0
> - Second channel: rtsp://Device's IP/live/ch00_1
> - The auxiliary camera at the device bottom: rtsp://Device's IP/live/ch00_2

RTSP OSD Setting

This feature is used to add a watermark to the RTSP video or picture.

Set it up on the web **Surveillance > RTSP > RTSP OSD Setting** interface. It is disabled by default.
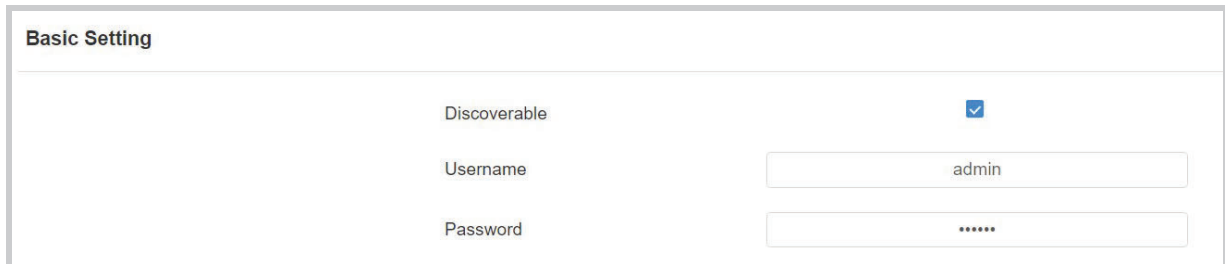

- **OSD Color**: There are five color options, White, Black, Red, Green, and Blue, for RTSP watermark text.
- **Top Text**: Customize the watermark text displayed at the top.
- **Bottom Text**: Customize the watermark text displayed at the bottom.

ONVIF

You can access the real-time video from the device's camera using the Akuvox indoor monitor or other third-party devices like Network Video Recorder(**NVR**). Enabling and setting up the ONVIF function on the device will allow its video to be visible on other devices.

Click here to view an example of using the ONVIF feature: the integration with Uniview NVR System.

To set it up, go to the web **Surveillance> ONVIF** interface.

Basic Setting

Discoverable	☑
Username	admin
Password	••••••

- **Discoverable**: When enabled, the video from the door phone camera is searchable by other devices.
- **Username**: Set the username required for accessing the door phone's video stream on other devices. It is admin by default.
- **Password**: Set the password required for accessing the door phone's video stream on other devices. It is admin by default.

> **Tip**
>
> Once the settings are configured, to access the video stream on the third-party device, simply enter the ONVIF URL: http://Device's IP:80/onvif/device_service.

Some NVRs can send door-opening requests to the device and control door opening. You can enable or disable the function by turning on or off a switch on the same interface as the ONVIF feature.

Advanced Setting

Milestone VMS Enabled	☐

Video Record

The video record feature enables the device to record videos automatically when specific events happen.

Except for package detection, the X910 only uses the main camera to record videos.

Set it up on the **Surveillance > Video Record** interface.

- **File Storage**: Store the videos in the SD Card or the SmartPlus Cloud. Only when the device has an SD card inserted or is connected to the SmartPlus Cloud will these two options display. When videos are stored in the SD card, the storage path is **date/event/event details**.

- **Video Length**: The video recording length.
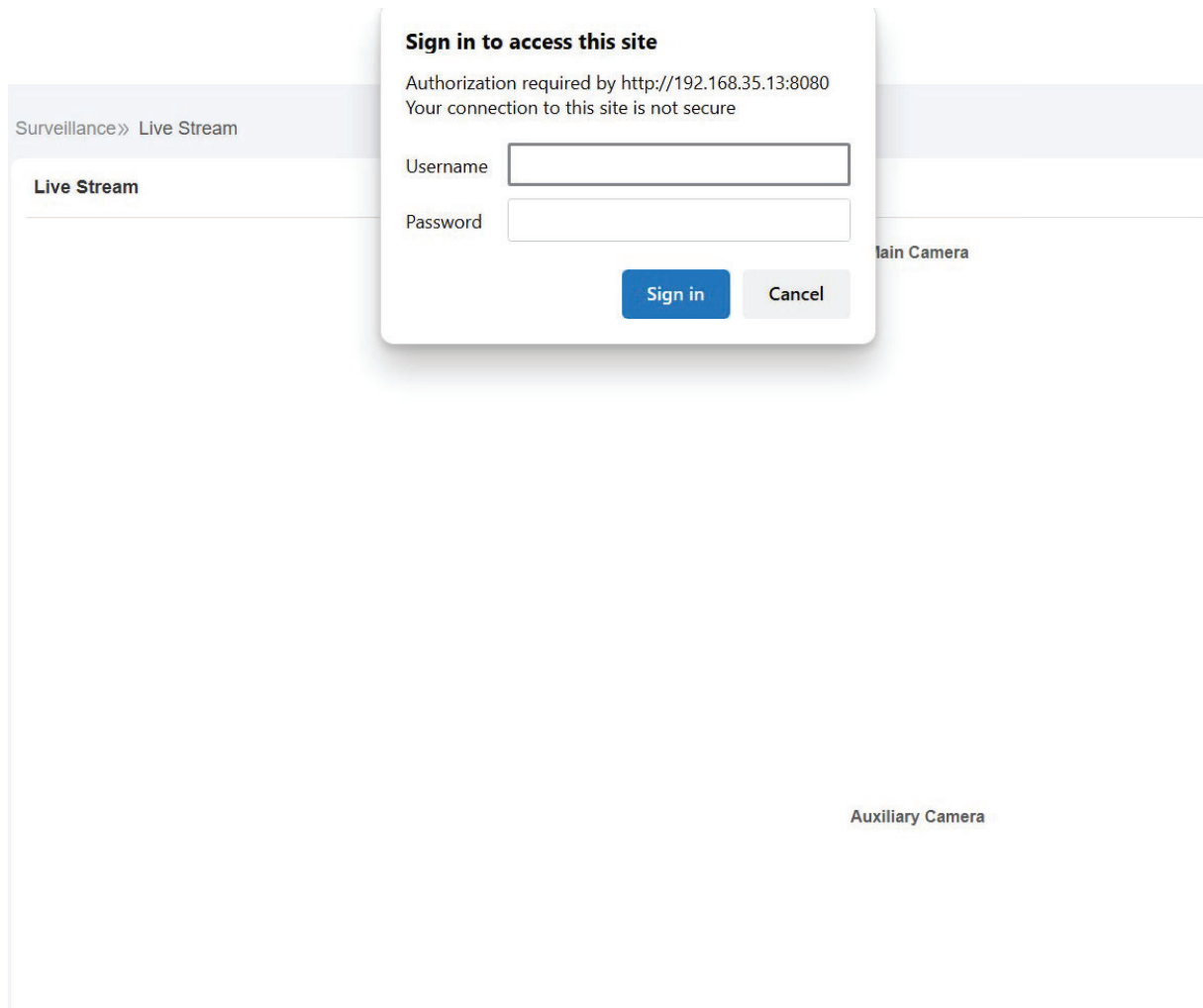- **Event Type**: Specify the event that will trigger video recording.

> **Note**
>
> - When the videos are stored in the SD card, all event types are supported.
> - When the videos are stored on the SmartPlus Cloud, specific event types(Access Granted/Denied; Motion Detected; Call Incoming/Outgoing) are supported.
> - Click **here** to view how to set up the feature on the SmartPlus Cloud.

Live Stream

There are two ways to check the real-time video from the device. One is to go to the device web interface and view the video there. The other is to enter the correct URL on the web browser and access the video directly.

View the video stream on the **Surveillance > Live Stream** interface. If you have enabled MJPEG authorization, you need to enter the user name and password set in the RTSP Basic section for viewing the stream.

Surveillance » Live Stream

Live Stream

Sign in to access this site

Authorization required by http://192.168.35.13:8080
Your connection to this site is not secure

Username

Password

Sign in   Cancel

Main Camera

Auxiliary Camera

NACK

Negative Acknowledgment（**NACK**）indicates a failure or error in data transmission or processing. It is used to request retransmission or signal the failure to the sender for ensuring data integrity.

To enable NACK, navigate to the web **Intercom > Call Feature > Others** interface.

Others

NACK Enable ☑

Data Transmission Type for Third-party Camera

You can select the data transmission type between the device and a third-party camera when it is connected to the SmartPlus Cloud.

To set it up, go to the **Surveillance > RTSP > Third Party Camera** interface.

Third Party Camera

Transport Type | TCP ▼

- **UDP**: An unreliable but very efficient transport layer protocol.
- **TCP**: A less efficient but reliable transport layer protocol. It is the default transport protocol.

SD Card for Storing Videos

The device can be inserted into an SD card to store motion and call videos.

To check the videos, go to **Device > SD Card** interface. When there is not enough space in the SD card to record the next video, the system automatically deletes the oldest video.

Files

ROOT [Back]

☐	Name ⇵	Type	Time ⇵	Action
☐ 📁	backups	Folder	Mon Jul 24 19:07:50 2017	[Download] [Delete]
☐ 📁	baidu	Folder	Mon Jul 24 19:10:44 2017	[Download] [Delete]
☐ 📁	bluetooth	Folder	Mon Apr 19 12:34:14 2021	[Download] [Delete]
☐	changba_log631.txt	File	Sun Aug 2 16:33:34 2015	[Download] [Delete]
☐ 📁	com.sina.weibo	Folder	Mon Jul 25 09:48:58 2016	[Download] [Delete]
☐ 📁	data	Folder	Thu Aug 6 11:37:46 2015	[Download] [Delete]
☐ 📁	documents	Folder	Sat May 18 09:53:04 2019	[Download] [Delete]
☐ 📁	download	Folder	Tue Dec 6 23:35:30 2016	[Download] [Delete]
☐ 📁	dq_advertise	Folder	Thu Oct 20 23:52:48 2016	[Download] [Delete]
☐ 📁	emlibs	Folder	Mon Oct 3 21:10:30 2016	[Download] [Delete]

[🗑 Delete] [🗑 Delete All] [Download] [Download All] [Prev] 11/16 [Next] [1] [Go]

You can backup the door phone's configuration data to the SD card and restore it from the SD card.

Backup & Restore

Backup Data	↻ Backup
Restore Data	↻ Restore

Camera Mode

- High Dynamic Range (HDR) is a technology used in photography, videography, and display devices to enhance image quality by capturing a wider range of brightness and color.
- Linear refers to a straightforward representation of brightness in images. Linear images are commonly used in controlled lighting environments, such as indoor scenes, where consistent brightness is present.

You can set the camera mode between HDR and Linear on the **Device > Camera** interface. It is HDR by default.

HDR

Enabled	☑

Linear

Anti-Flicker Mode	Auto ▼
Anti-Flicker Frequency	50HZ ▼

Camera Setting

Sensor Framerate	25fps ▼

- **Anti-Flicker Mode**: The anti-flicker feature reduces or eliminates flickering in images or videos caused by varying light sources.
    - **Auto**: The device will switch automatically between 50Hz and 60Hz anti-flicker frequency.
    - **Manual**: Select the anti-flicker frequency manually.
    - **Off**: Disable the anti-flicker function.
- **Anti-Flicker Frequency**: Select the anti-flicker frequency between 50Hz and 60Hz.
- **Sensor Framerate**: Adjust the camera frame rate.
    - **30fps**: Better for applications needing higher smoothness.
    - **25fps**: Suitable for standard video recording and playback, especially under a 50Hz power frequency to minimize flicker.

Package Detection

The door phone can send notifications or open doors when its auxiliary camera(at the device's bottom) detects packages.

Set this feature on the **Surveillance > Package** interface. It is disabled by default.

- **Detection Area**: You can click and hold the mouse button to select up to three detection areas. When packages are detected within these three areas, the preset actions will be carried out.
- **Detection Accuracy**: Select the accuracy level between 1 and 2. Higher value indicates a higher accuracy. The default is 1.
- **Action to Execute**: Set the desired actions that occur when package detection is triggered.
    - **FTP**: Send a screenshot to the preconfigured FTP server.
    - **Email**: Send a screenshot to the preconfigured Email address.

- **SIP Call**: Call the preset number upon the trigger.
- **HTTP**: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP and enter the URL.
- **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
- **Execute Relay**: Specify the relay to be triggered.

You can set the schedule that determines when the feature is effective on the **Package Detect Time Setting** part.

Package Detect Time Setting

Day	☑ Mon	☑ Tue	☑ Wed
	☑ Thur	☑ Fri	☑ Sat
	☑ Sun	☐ Check All	

Start Time - End Time	00:00 🕐	-	23:59 🕐

Security

Tamper Alarm

The tamper alarm function prevents anyone from removing the device without permission. Akuvox devices support two types of tamper proof: gravity detection and button status detection.

Click here to view which type is supported by the device and learn the function details.

To set it up, go to **System > Security > Tamper Alarm** interface.

- **Disarm**: Click Disarm to clear the arming.

Client Certificate Setting

Certificates ensure communication integrity and privacy. To use the SSL protocol, you need to upload the right certificates for verification.

Web Server Certificate

It is a certificate sent to the client for authentication when the client requests an SSL connection with the Akuvox door phone. Please upload the certificates in accepted formats.

Upload Web Server Certificate on the web **System > Certificate** interface.

Client Certificate

This certificate verifies the server to the Akuvox door phone when they want to connect using SSL. The door phone verifies the server's certificate against its client certificate list.

Upload and configure the Client Certificate on the **System > Certificate** interface.

- **Index:**
  - Auto: The uploaded certificate will be displayed in numeric order.
  - 1 to 10: the uploaded certificate will be displayed according to the value selected.
- **Upload:** Click Choose File to upload the certificate.
- **Only Accept Trusted Certificates:** When enabled, as long as the authentication succeeds, the doorphone will verify the server certificate based on the client certificate list. If select Disabled, the doorphone will not verify the server certificate no matter whether the certificate is valid or not.

Motion Detection

Motion Detection is a feature that allows unattended video surveillance and automatic alarms. It detects any changes in the image captured by the camera, such as someone walking by or the lens being moved, and activates the system to perform the appropriate action.

Set up motion detection on the **Surveillance > Motion** interface.

Motion Detection Options

Suspicious Moving Object Detection	Radar Detection ▼	
Time Interval	10	(0~120Sec)
Detection Range	3 ▼	(m)

Motion Action

Action To Execute	☐ FTP ☐ Email ☐ SIP Call ☐ HTTP	
Execute Relay	None ▼	

- **Suspicious Object Movement Detection:** The feature uses the main camera for detection.
    - **Disabled**: Turn off the feature.
    - **Video Detection**: When the video camera detects moving objects, preset actions will be triggered. Focus on analyzing visual information captured through cameras.
    - **Radar Detection**: When the radar detects moving objects, preset actions will be triggered. It offers longer-range and better detection in poor visibility conditions.
    - **Video + Radar**: Detect motion with the combination of video camera and radar.
    - **Pedestrian Detection**: When the device detects the upper body of the passers-by, preset actions will be triggered.
    - **Pedestrian + Radar**: Combine the pedestrian and radar detection.
- **Time Interval:** If the default time interval for motion detection is set to 10 seconds, the detection period lasts the same duration. The first detected movement marks the start, and if movement persists for 7 seconds within this interval, the alarm triggers at 7 seconds, with notifications sent between 7 and 10 seconds.
- **Detection Accuracy**: Not available for radar detection. The detection sensitivity. The higher the value, the greater the sensitivity. The default detection accuracy value is 3.
- **Detection Range**: Set the distance within which radar detection is triggered. The range includes 1, 2, and 3 meters.
- **Detection Area**: Click and hold the mouse button to select up to three detection areas. When motion is detected within these areas, preset actions will be carried out.
- **Action To Execute**: Set the desired actions that occur when suspicious movement is detected.

- FTP: Send a screenshot to the preconfigured FTP server.
- Email: Send a screenshot to the preconfigured Email address.
- SIP Call: Call the preset number upon the trigger.
- HTTP: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
  - **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
  - **Execute Relay**: A relay can be unlocked with motion detection.

Scroll down and you can set the motion detection schedule.

Security Notification

A security notification informs users or security personnel of any breach or threat that the device detects. For example, if the device detects something unusual, the system sends a notification to users or security through email, phone calls, or other methods.

To set up security notifications, go to **Setting > Action** interface.

Email Notification

Set up email notifications to receive screenshots of unusual motion from the device.

Click here to view how to set this feature up.

Set it up in the **Email Notification** section.

Email Notification

Sender Email Address	
Receiver Email Address	
SMTP Server Address	
SMTP User Name	
SMTP Password	••••••
Email Subject	
Email Content	
Email Test	↻ Test

- **SMTP Server Address**: The SMTP server address of the sender.
- **SMTP Username**: The SMTP username is usually the same as the sender's email address.
- **SMTP Password**: The password of the SMTP service is the same as the sender's email address.

FTP Notification

To get notifications through FTP server, you need to set up the FTP settings. The door phone will upload a screenshot to the specified FTP folder if it senses any unusual motion.

Click here to view the configuration steps.

Set it up in the **FTP Notification** section.

FTP Notification

FTP Server	
FTP User Name	
FTP Password	••••••
FTP Test	↻ FTP Test

- **FTP Server:** Set the address (URL) of the FTP server.
- **FTP Username**: Enter the user name to access the FTP server.
- **FTP Password**: Enter the password to access the FTP server.

SIP Call Notification

In addition to FTP and Email notification, the door phone can also make a SIP call when some feature action is triggered.

Set it up in the **SIP Call Notification** section.

SIP Call Notification

Number	
Display Name	

- **Display Name**: The name of the device displayed in the notification.

Action URL

You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status, input status, PIN code, or RF card access changes.

Akuvox Action URL:

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

For example: http://192.168.16.118/help.xml? mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn

To set it up, go to the **Setting > Action URL** interface.

Action URL

Enabled	☐
Type	GET ▾
User Name	
Password	••••••
Make Call	
Hang Up	
RelayA Triggered	
RelayB Triggered	
RelayA Closed	
RelayB Closed	
InputA Triggered	
InputB Triggered	
InputA Closed	
InputB Closed	
Valid Card Entered	
Invalid Card Entered	
Break In Alarm A	
Break In Alarm B	

- **Enabled**: When enabled, you can select the schedule within which the action URL can be performed.
- **Type**: Select the request type between GET and POST.

Voice Encryption

Secure Real-time Transport Protocol (SRTP) is a protocol derived from the Real-time Transport Protocol (RTP). It enhances the security of data transmission by providing encryption, message authentication, integrity assurance, and replay protection.

Set it up on the web **Account > Advanced > Encryption** interface.

Encryption

Voice Encryption(SRTP)	Disabled ▼

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

User Agent

User agent is used for identification purpose when you are analyzing the SIP data packet.

To set it up, navigate to the **Account > Advanced > User Agent** interface.

User Agent

User Agent	

- **User Agent:** Akuvox is by default.

Real-Time Monitoring

This feature displays the door status when the device is connected to the SmartPlus Cloud. Property managers and end users can check the door status respectively on the SmartPlus Property Manager platform and SmartPlus App.You need to specify the relay(s) or input(s) that apply this feature. Click here to see the detailed configuration.

To set it up, go to **System > Security > Real-Time Monitoring** interface.

Real-Time Monitoring

Apply Setting To	None ▼

- **Apply Setting To**:
  - **None**: Not display door status.
  - **Input**: The door is opened by triggering input.
  - **Relay**: The door is opened by triggering the relay.

Emergency Action

This feature works with Akuvox SmartPlus Cloud. It keeps the door open when an emergency happens. You need to specify the Input that applies the feature.

Click here to view the detailed configuration of this feature.

To set it up, go to **System > Security > Emergency Action** interface. Select the Input(s) to be triggered.

Emergency Action

Apply Setting To	☐ Input A ☐ Input B

Web Interface Automatic Log-out

You can set up the web interface's automatic log-out timing, requiring re-login by entering the user name and the passwords for security purposes or for the convenience of operation.

To set it up, go to **System > Security > Session Time Out** interface.

Session Time Out

Session Time Out Value	9000	(60~14400Sec)

High Security Mode

High security mode is designed to enhance the security. It employs encryption across various facets, including the communication process, door opening commands, password storage methods, and more.

Enable it on the **System > Security > High Security Mode** interface.

High Security Mode

Enabled	☑

Important Notes

1. The High Security mode is off by default when you upgrade the device from a version without the mode to one with it. But if you reset the device to its factory settings, the mode is on by default.

2. This mode makes the old version tools incompatible. You need to upgrade them to the following versions or higher to use them.

- PC Manager: 1.2.0.0
- IP Scanner: 2.2.0.0
- Upgrade Tool: 4.1.0.0
- SDMC: 6.0.0.34

3. The supported HTTP format for relay triggering varies depending on whether high secure mode is enabled or disabled.

If the mode is on, the device only accepts the new HTTP formats below for door opening.

- http://username:password@deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1
- http://deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1

If the mode is off, the device can use both the new formats above and the old format below:

- http://deviceIP/fcgi/do?action=OpenDoor&UserName=username&Password=password&DoorNum=1

4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

Logs

Call Logs

To check calls—including dial-out, received, and missed calls—within a specific period, you can view the call log on the device's web interface. If needed, you can also export the call log from the device.

Check call logs on the web **Status > Call Log** interface. You can export call logs in a CSV file by clicking **Export**. The device supports up to 1,000 call logs.

Call Log

	Index	Type	Date	Time	Local Identity	Name	Number	Action
☐	1	Received	2024-12-27	15:10:18	5926100323@pbx.test.akuvox.com	P M	5926100289@pbx.test.akuvox.com	Picture
☐	2	Received	2024-12-27	14:59:03	5926100322@pbx.test.akuvox.com	testest	5926100285@pbx.test.akuvox.com	Picture
☐	3	Dialed	2024-12-27	14:48:38	5926100322@pbx.test.akuvox.com	Reception	19253165@pbx.test.akuvox.com	Picture
☐	4	Received	2024-12-27	14:47:54	5926100322@pbx.test.akuvox.com	testest	5926100285@pbx.test.akuvox.com	Picture
☐	5	Received	2024-12-27	14:47:23	192.168.35.18@192.168.35.18	R29	192.168.35.29@192.168.35.29	Picture

Save Call Log Enabled ☑
Save Picture Enabled ☑
Export Picture Enabled ☐

All · Start Time ~ End Time · Name/Number · Search · Export ▾

- **Save Picture Enabled**: When enabled, the device will capture pictures of calls, and you can click Picture in the Action column to view the screenshot.
- **Export Picture Enabled**: Set whether to export the captured images when exporting the call logs.
- **Call History:** There are four specific types of call logs: All, Dialed, Received, and Missed.
- **Start Time - End Time:** Search the desired call log by entering a certain period.
- **Name/Number:** Search the desired call log by entering the name and number.
- **Picture**: Click to view the snapshot during a call.

Door Logs

To search and review various types of door access history, simply check the door logs on the device's web interface.

Check door logs on the **Status > Access Log** interface. You can export logs in a CSV or XML file by clicking Export. The device supports up to 5,000 door logs.

- **Save Picture Enabled**: When enabled, the device will capture pictures of the door opening, and you can click Picture in the Action column to view the screenshot.
- **Export Picture Enabled**: Set whether to export the captured images when exporting the door logs.
- **Status:** Display Successful and Failed door-opening records.
- **Start Time - End Time:** Search the desired call log by entering a certain period.
- **Name:** Display user name. If it is an unknown key or card, it will display Unknown.
- **Code:** If the door is opened by RF cards, the card code will be displayed. If the door is opened by an HTTP command, it will be empty.
- **Type:** Display the access methods.
- **Picture**: Click to view the snapshot when the door opens.

Integration with Third Party Device

Integration via Wiegand

The Wiegand feature enables the Akuvox device to act as a controller or a card reader.

Set it up on the web **Device > Wiegand > Wiegand** interface.

Wiegand

Wiegand Display Mode	8HN ▼
Wiegand Card Reader Mode	Auto
Wiegand Transfer Mode	Input ▼
Wiegand Input Data Order	Normal ▼

- **Wiegand Display Mode**: Select the Wiegand card code format from the provided options.
- **Wiegand Card Reader Mode**: It is automatically configured when **Input** is the Wiegand Transfer Mode. If Output is the Wiegand Transfer Mode, the transmission format should be identical between the door phone and the third-party device.
- **Wiegand Transfer Mode**:
    - **Input**: The device serves as a receiver.
    - **Output**: The device serves as a sender and can directly output the data, such as card code.
    - **Convert To Card No. Output**: The device serves as a sender and cannot directly output data, such as the face data.
- **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.
- **Wiegand Output Data Order:** Determine the sequence of the card data after the Wiegand conversion.
  For example, if the card data is 0x11 0x22 0x33 0x44 0x55, it will be 0x33 0x44 0x55 after the Wiegand conversion(e.g., Wiegand 26). If **Reversed** is selected, the card data is 0x55 0x44 0x33.

- **Wiegand Output Basic Data Order**: Set the sequence of the card data before going through Wiegand conversion and outputting the card code.
  For example, if the card data is 0x11 0x22 0x33 0x44 and the **Reversed** option is selected, the data will be 0x44 0x33 0x22 0x11.
- **Wiegand Output CRC Enabled**: It is enabled by default for Wiegand data inspection. Disabling it may lead to integration failure with third-party devices.

> **Note**
>
> Click **here** to view more information on Wiegand settings including:
>
> - Akuvox devices work as Wiegand input/output;
> - Wiegand Card Reader Connection.

Integration via HTTP API

HTTP API is designed to achieve a network-based integration between the third-party device and the Akuvox device.

Set it up on the web **Setting > HTTP API** interface.

- **Enabled**: Enable or disable the HTTP API function for third-party integration. If the function is disabled, any request to initiate the integration will be denied and return HTTP 403 forbidden status.

- **Authorization Mode**: It is Digest by default. You are required to fill in the username and password for the authentication. In the Authorization field of the HTTP request header, use the Base64 encode method to encode the username and password.
- **User Name**: Enter the user name for authentication. The default is admin.
- **Password**: Enter the password for authentication. The default is admin.
- **1st IP-5th IP**: Enter the IP address of the third-party devices when the **Allowlist** authorization is selected for the integration.

Please refer to the following description for the authentication mode:

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

Integration via RS485

You can connect the device to an external device such as SR01 or an OSDP-based card reader via RS485. To make the connection effective, you need to select the right RS485 mode.

Click here to view the detailed configuration of the OSDP feature.

To set it up, go to the **Device > RS485** interface.

RS485 Setting

Apply RS485 Setting To	OSDP ▼

OSDP Setting

Encryption	☐
TransferMode	Input ▼
SCBK Value	

- **Apply RS485 Setting To**:
  - **Disabled**: The RS485 function is disabled.
  - **OSDP**: The device is connected to an OSDP-based external device such as a card reader.
  - **Security Relay**: The device is connected to Akuvox Security Relay, SR01.
- **Encryption**: Check this option when the protocol is encrypted.
- **Transfer Mode**: Select the RS485 working mode, Output, or Input.
- **SCBK Value**: Secure Communication Key Value.
  - When it is filled, OSDP will use this value for encryption, employing a customized protocol for communication.
  - When it is left empty, OSDP will use the default encrypted protocol for communication.

Power Output Control

The device can serve as a power supply for the external relays.

To set it up, go to **Access Control > Relay > 12V Power Output** interface.

12V Power Output

Relay ID	RelayA
Power Output Type	Disabled ▼

- **Power Output Type**:
    - **Always**: Provide continuous power to the third-party device.
    - **Triggered by Open Relay**: Provide power to the third-party device via 12 output and GND interface during the timeout when the status of relays is shifted from low to high.

Lift Control

The device can be connected to the Akuvox lift controller for the lift control. Users can summon the lift to go down to the ground floor when they are granted access through various types of access methods on the device.

Click here to watch a demonstration video of configuring the lift control feature.

To set it up, go to the **Device > Lift Control** interface. Select **Akuvox** for integration with the Akuvox EC33 lift controller.

General Setting

Server 1 IP (Unlock)	
Port	
Server 2 IP (Execute)	
Port	

Action Setting

User Name	
Password	••••••
Floor No. Parameter	$floor
URL To Trigger Specific Floor	/cdor.cgi?open=0&door=$floor
URL To Trigger All Floors	/cdor.cgi?open=8
URL To Close All Floors	/cdor.cgi?open=9
Floor Starts From	1 ▼
Device Location	None ▼

- **Server 1 IP(Unlock)**: The IP address of the lift controller that unlocks the elevator button(s). It supports up to 10 server addresses separated by ";".
- **Server 2 IP(Execute)**: The IP address of the lift controller that sends the lift control commands.
- **Port**: The server port of the lift controller server.

- **User Name**: The username of the lift controller for the authentication.
- **Password**: The password of the lift controller for the authentication.
- **Floor NO. Parameter**: Enter the floor number parameter provided by Akuvox. The default parameter string is "$floor". You can define your parameter string if needed.
- **URL To Trigger Specific Floor**: Enter the Akuvox lift control URL for triggering a specific floor. The URL is /cdor.cgi?open=0&door=$floor, but the string "$floor" at the end must be identical to the parameter string you defined.
- **URL To Trigger All Floors**: Enter the Akuvox URL for triggering all floors.
- **URL To Close All Floors**: Enter the Akuvox URL used for closing all floors, meaning all the buttons that are triggered for the corresponding floors will become invalid.
- **Floor Starts From**: Set the floor from which the floor count starts. For example, if you select -3, then the 3rd floor in the basement will be considered as the first floor, matched with relay#1 (first floor).
- **Device Location**: Select the floor where the device is installed.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

To upgrade the device, go to **System > Upgrade** interface.

Basic

Firmware Version	2910.30.10.240
Hardware Version	2910.2
Upgrade	⇥ Upgrade
Reset To Factory Setting	↻ Reset
Reset Configuration To Default State	↻ Reset
Reboot	⏻ Reboot

> **Note**
> Firmware files should be in **.rom** format for upgrade.

Auto-provisioning via Configuration File

You can configure and upgrade the device through the web interface using one-time or scheduled auto-provisioning with configuration files. This eliminates the need to set up configurations manually, saving you time and effort.

Provisioning Principle

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

Please see the flow chart below:
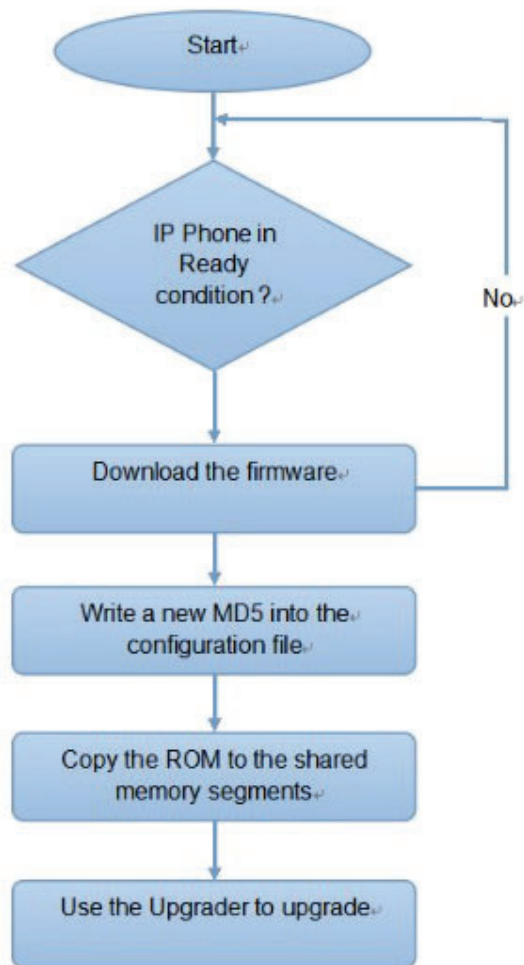
Configuration Files for Auto-provisioning

Configuration files for auto-provisioning come in two formats: general configuration files and MAC-based configuration files.

Differences:

- **General Configuration Provisioning**:

A general configuration file is stored on a server, allowing all related devices to download the same file to update parameters.

- **MAC-Based Configuration Provisioning**:

MAC-based configuration files are specific to individual devices, identified by their unique MAC addresses. Files named with the device's MAC address will be matched automatically before downloading for provisioning.

> **Note**
>
> - Configuration files must be in CFG format.
> - The name of the general configuration file for batch provisioning varies by model.
> - The MAC-based configuration file is named after its MAC address.
> - Devices will first access general configuration files before the MAC-based ones if both types are available.
>
> You may click **here** to see the detailed format and steps.

AutoP Schedule

Akuvox provides you with different AutoP methods that enable the device to perform provisioning for itself according to the schedule.

To set it up, go to the web **System > Auto Provisioning > Automatic AutoP** interface.
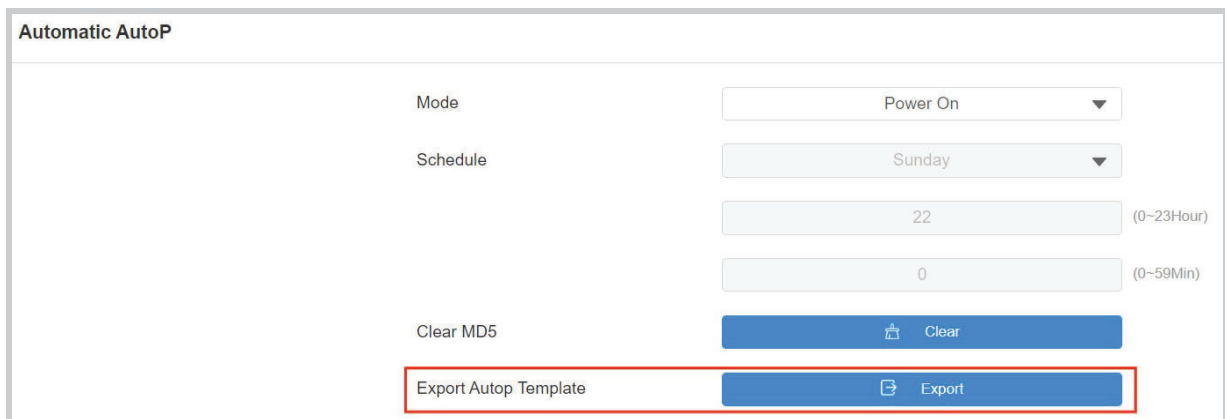
Automatic AutoP		
Mode	Power On	▼
Schedule	Sunday	▼
	22	(0~23Hour)
	0	(0~59Min)
Clear MD5	🗑 Clear	
Export Autop Template	↪ Export	

- **Mode**:
  - **Power On**: The device will perform Autop every time it boots up.
  - **Repeatedly**: The device will perform Autop according to the schedule you set up.
  - **Power On + Repeatedly**: 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**: The device will perform Autop every hour.

Static Provisioning

You can manually set up a specific server URL for downloading the firmware or configuration file. If an auto-provision schedule is set up, the device will perform the auto-provisioning at a specific time according to the auto provision schedule you set up. In addition, TFTP, FTP, HTTP, and HTTPS are the protocols that can be used for upgrading the device firmware and configuration.
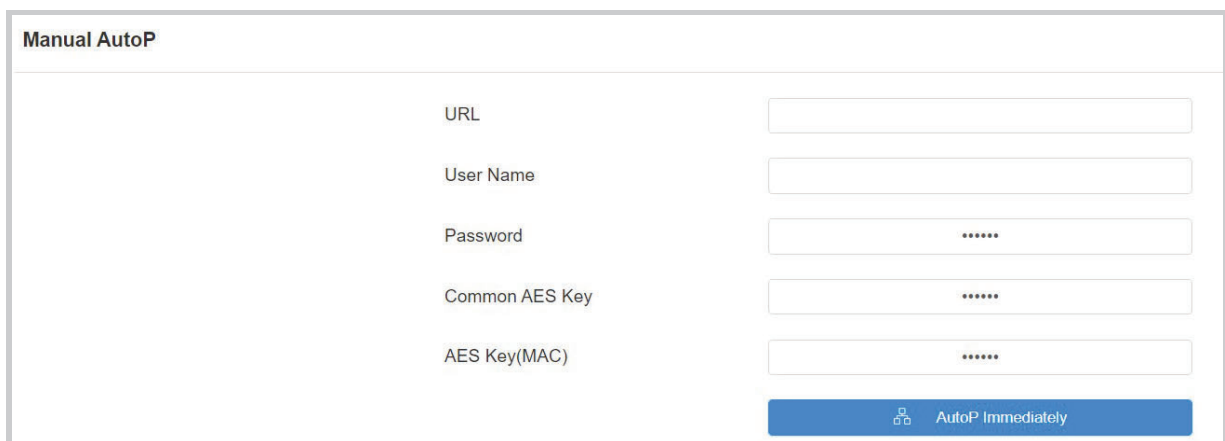
To set it up, download the template on **System > Auto Provisioning > Automatic AutoP** interface first.

Set up the Autop server in the **Manual AutoP** section.

- **URL**: Specify the TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **Username**: Enter the username if the server needs a username to be accessed.
- **Password**: Enter the password if the server needs a password to be accessed.
- **Common AES Key**: It is used for the intercom to decipher general Autop configuration files.

- **AES Key (MAC)**: It is used for the intercom to decipher the MAC-based Autop configuration file.

> **Note**
>
> - AES as one type of encryption should be configured only when the config file is encrypted with AES.
> - 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 does not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

DHCP Provisioning

Auto-provisioning URL can also be obtained using the DHCP option which allows the device to send a request to a DHCP server for a specific DHCP option code. If you want to use **Custom Option** as defined by users with option codes ranging from 128-255), you are required to configure DHCP Custom Option on the web interface.
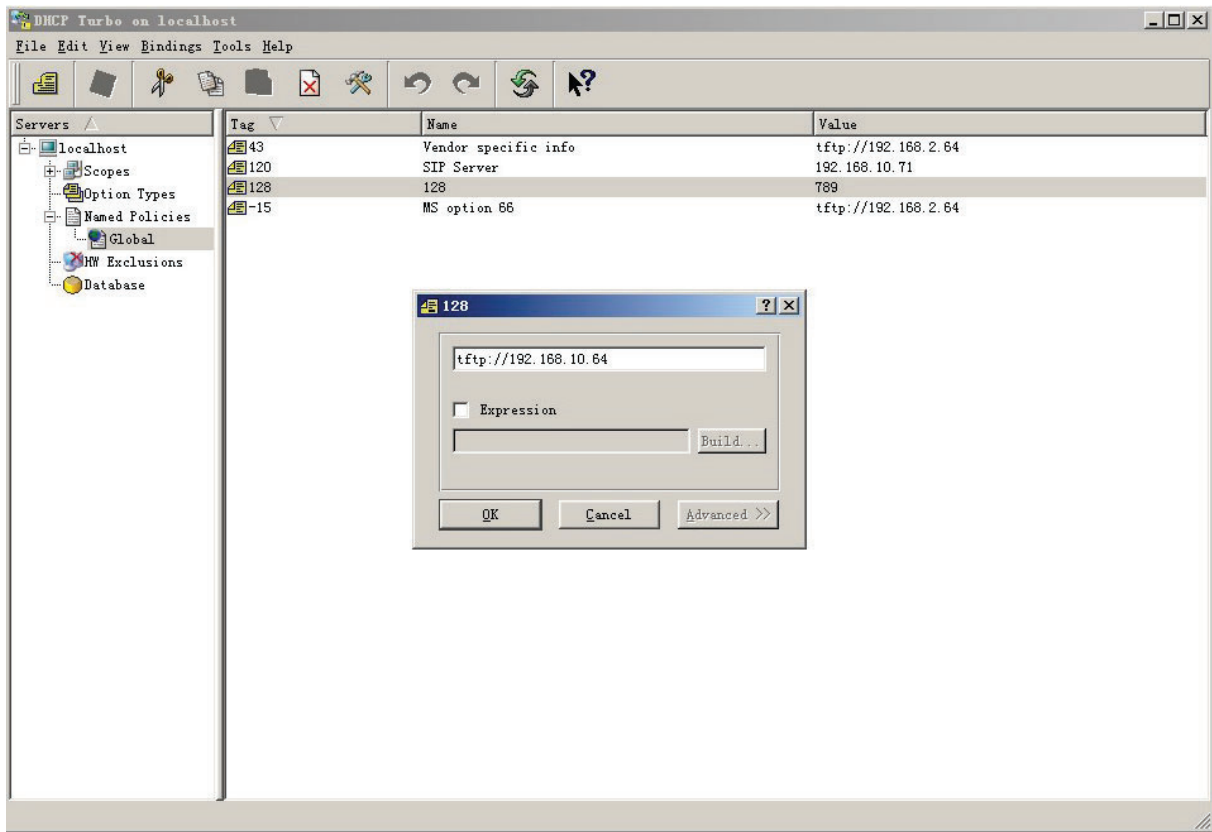
Note

The Custom Option type must be a string. The value is the URL of the TFTP server.

Set up DHCP Autop with Power On mode and export Autop Template to edit the configuration.

Download the Autop template on the **System > Auto Provisioning > Automatic AutoP.**
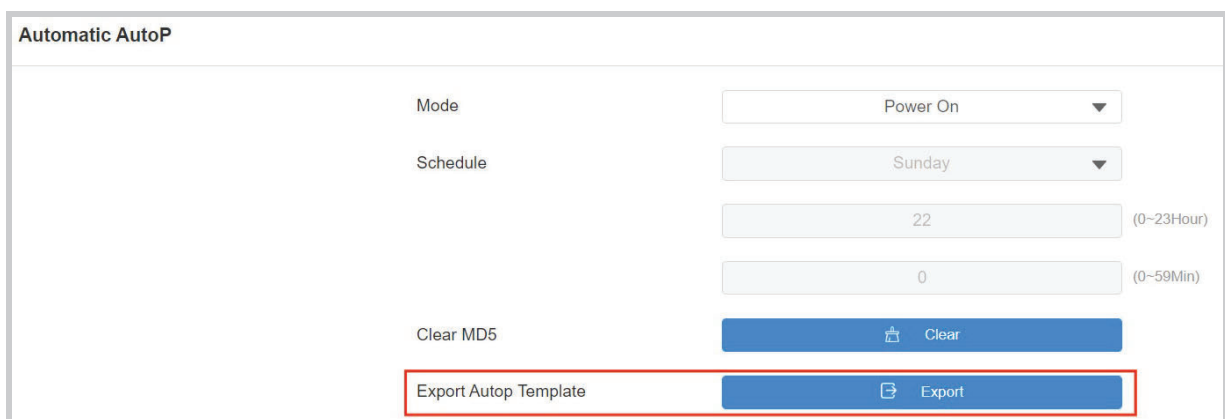
Set it up on **System > Auto Provisioning > DHCP Option** interface.

DHCP Option

Custom Option	[ ] (128~254)

(DHCP Option 66/43 is Enabled by Default)

- **Custom Option**: Enter the DHCP code that matches the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 66**: If none of the above is set, the device will automatically use DHCP Option 66 to get the upgrade server URL. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 66 with the updated server URL in it.
- **DHCP Option 43**: If the device does not get a URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 43 with the updated server URL in it.

PNP Configuration

Plug and Play (PNP) is a combination of hardware and software support that enables a computer system to recognize and adapt to hardware configuration changes with little or no intervention by a user.

Click here to watch the configuration video.

Set it up on the web **System > Auto Provisioning > PNP Option** interface.
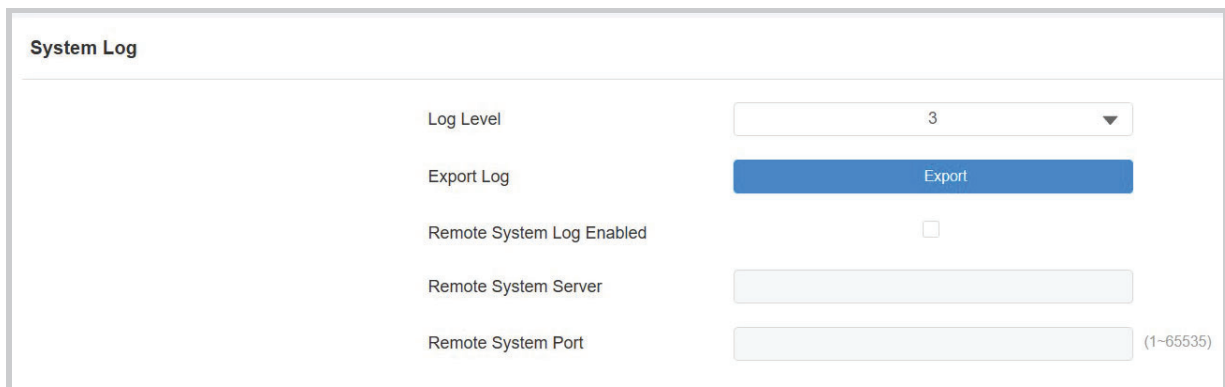
PNP Option

PNP Config Enabled	☑

Debug

System Log for Debugging

System logs can be used for debugging purposes.

To set it up, go to the web **System > Maintenance > System Log** interface.

- **Log Level:** Select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log:** Click the Export tab to export a temporary debug log file to a local PC.
- **Remote System Server:** Set the remote server address to receive the device log. The remote server address will be provided by Akuvox technical support.
- **Remote System Port**: Set the remote system server's port.

Remote Debug Server

When the device is having a problem, you can use the remote debug server to access the device log remotely for debugging purposes.

To set it up, go to the **System > Maintenance > Remote Debug Server** interface.

- **Connect Status**: Display the connection status between the device and the server.
- **Server IP**: Enter the IP address of the server.
- **Server Port**: Enter the port of the server.

PCAP for Debugging

PCAP is used to capture the data package going in and out of the devices for debugging and troubleshooting purposes.

To set it up, go to the web **System > Maintenance > PCAP** properly before using it.

- **Specific Port:** Select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** Click the Start tab and Stop tab to capture a certain range of data packets before clicking the Export tab to export the data packets to your Local PC.
- **PCAP Auto Refresh Enabled:** If it is enabled, then the PCAP will continue to capture data packets even after the data packets reach their 1M maximum in capacity. If it is disabled, the PCAP will stop data packet capturing when the data packet captured reaches the maximum capturing capacity of 1 MB.
- **New PCAP:** Click Start to capture a bigger data package.

Ping

The device allows you to verify the accessibility of the target server.

To set it up, go to **System > Maintenance > Ping** interface.
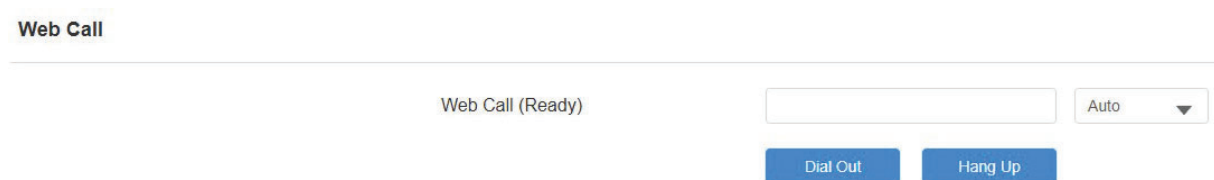
- **Cloud Server**: Select the server to be verified.
- **Verify the network address accessibility**: The service type includes TCP connection, FTP service, SIP service, etc. You can select the service type or enter it manually.

Web Call

The web call feature allows for making calls via the device's web interface, commonly used for remote call testing purposes.

Make a web call on **System > Maintenance > Web Call** interface.

- **Web Call (Ready):** Enter the target IP/SIP number and select the account to dial out.

Backup

You can import or export encrypted configuration files to your Local PC.

Export the file on the **System > Maintenance** interface. The imported file should be in the .tgz/.conf/.cfg format.

Others

Config File   [⇥ Import]   [↦ Export]   (Encrypted)

Backup via SD Card

The device supports inserting an SD card for backing up and restoring data.

To use this feature, go to **Device > SD Card** interface. The tested SD card capacity is 64GB.

Backup & Restore

Backup Data   [↺ Backup]

Restore Data   [↺ Restore]

Password Modification

You can modify the device web password for both the administrator account and the user account.

To set it up, go to **System > Security > Web Password Modify** interface.

Click **Change Password** to modify the password.

To enable or disable the user account, scroll to the **Account Status** section. The default password for the user account is **user**.

Modify Security Questions

Security questions allow you to reset the web password if you forget it. After setting up the security questions, you can click "Forget Password" on the login interface, enter the answers, and a password reset window will pop up.

If you do not set up the security questions, clicking "Answer security questions" will prompt you to "Please contact your service provider".

To set it up, go to **System > Security > Web Password Modify** interface.

Web Password Modify

User Name	admin ▼	🔒 Change Password
	⚙ Modify Security Question	

You are required to fill in the current password before modifying the security questions.

Web Password Modify

User Name   admin ▼   🔒 Change Password

Please set up your security questions.   ✕

Question 1	-- Select One -- ▼
Answer	
Question 2	-- Select One -- ▼
Answer	
Question 3	-- Select One -- ▼
Answer	

Cancel   Submit

Account Stat

Tamper Alarm

High Security

System Reboot&Reset

Reboot

If you want to restart the device system, you can operate it on the device web. Moreover, you can set up a schedule for the device to be restarted.

Navigate to the **System > Upgrade** interface.

Basic

Firmware Version	2910.30.10.240
Hardware Version	2910.2
Upgrade	Upgrade
Reset To Factory Setting	Reset
Reset Configuration To Default State	Reset
Reboot	Reboot

To set up the schedule, go to the **System > Auto Provisioning** interface.

Reboot Schedule

Enabled	☑
Schedule	Every Day
	0 (0~23Hour)

Reset

The device provides two reset options:

- **Reset to Factory Setting**: Reset all data to the factory default.
- **Reset Configuration to Default State**: Retain the user data, such as the RF cards, face data, schedules, and call logs.

Reset the device on the web **System > Upgrade** interface.

Basic

Firmware Version	2910.30.10.240
Hardware Version	2910.2
Upgrade	⤓ Upgrade
Reset To Factory Setting	↺ Reset
Reset Configuration To Default State	↺ Reset
Reboot	⏻ Reboot

> **Tip**
>
> The device also support resetting via a physical button on its back.
>
> - Remove its back cover, insert a PIN into the hole and hold it for about 3 seconds.
> - The backlight of the card reader area and fill light will light up, and the device goes into factory reset and reboot.
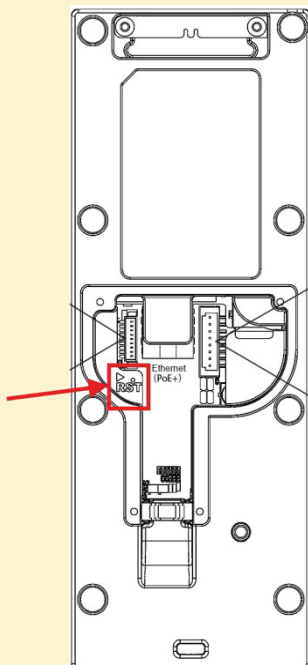
🛡️ FCC Caution:

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

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

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

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

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

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

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

FCC Radiation Exposure Statement:

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

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

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