Table of contents

Akuvox MR01 Millimeter Wave Radar Administrator Guide

About This Manual 3
Product Overview 4
Model Specification 5
Access the Device 6
Obtain Device IP Address 6
Access the Device Settings 6
Indicator Light Status 8
Turn on/off the LED 9
Introduction to the Configuration Menu 10
Language and Time 11
Language 11
Custom Language 11
Time 12
Daylight Saving Time 13
Network Setting 15
Check Network Information 15
Device Network Configuration 15
Wi-Fi Connection 16
Wi-Fi AP Setting 16
Device Deployment in Network 17
Device Local RTP Configuration 19
Device Web HTTP Setting 19
SNMP Setting 20
Fall Setting 21
Room Setting 21
Sub-region Setting 23
Room Status 26
Fall Detection Setting 28
Alarm Setting 29
Clear Alarm 29
Turn on/off Buzzer 30
Send Alarm Notification to Third-Party Server 30
Auto-provisioning 31
Introduction to the Configuration Files 31
AutoP Schedule 32

Static Provisioning Configuration 33
PNP Configuration 35
Firmware Upgrade 37
Security 38
Web Interface Automatic Log-out 38
High Security Mode 38
Backup 39
Debug 40
System Log for Debugging 40
PCAP for Debugging 40
Remote Debug Server 41
Point Cloud Data Export 41
Password Modification 43
Modify Device Web Interface Password 43
Modify Security Questions 44
System Reboot & Reset 45
Reboot 45
Reset 45

About This Manual

Thank you for choosing the Akuvox MR01 Millimeter Wave Radar. This manual is intended for administrators who need to properly configure the device. This manual applies to version 301.30.10.12. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview



MR01 (Millimeter Wave Radar) is an intelligent sensing device designed for fall detection in elderly care facilities, healthcare institutions, and similar indoor scenarios. It supports both fall detection and bed-exit detection to improve safety monitoring.

The device uses 4D millimeter-wave radar technology combined with AI algorithms to accurately detect human status with high accuracy and low false alarm rates. MR01 does not use a camera and does not require wearable devices, ensuring ease of use while protecting user privacy.

MR01 supports both ceiling and wall mounting for flexible installation. It can also integrate with the Akuvox Cloud, SDMC, indoor monitors, management stations, and third-party systems to report alarms for remote monitoring and centralized management.

Key Features:

- Fall detection and bed-exit detection
- 4D millimeter-wave radar with AI detection
- Camera-free design for privacy protection
- Flexible installation (ceiling or wall mounting)
- Alarm integration with Akuvox platforms and third-party systems

Model Specification

Model	MR01
Operation System	Linux
Power Input	Type-C or PoE
RJ45	1 × RJ45 (PoE supported)
Bluetooth	Bluetooth 5.0 or above
Wi-Fi	802.11 b/g/n/ac/ax (2.4 GHz / 5 GHz)
Relay Interface	x1
Physical Button	x1, for IP annoucement
Reset Button	x1
LED Indicator	x1
Reset Button	✔
Speaker	x1

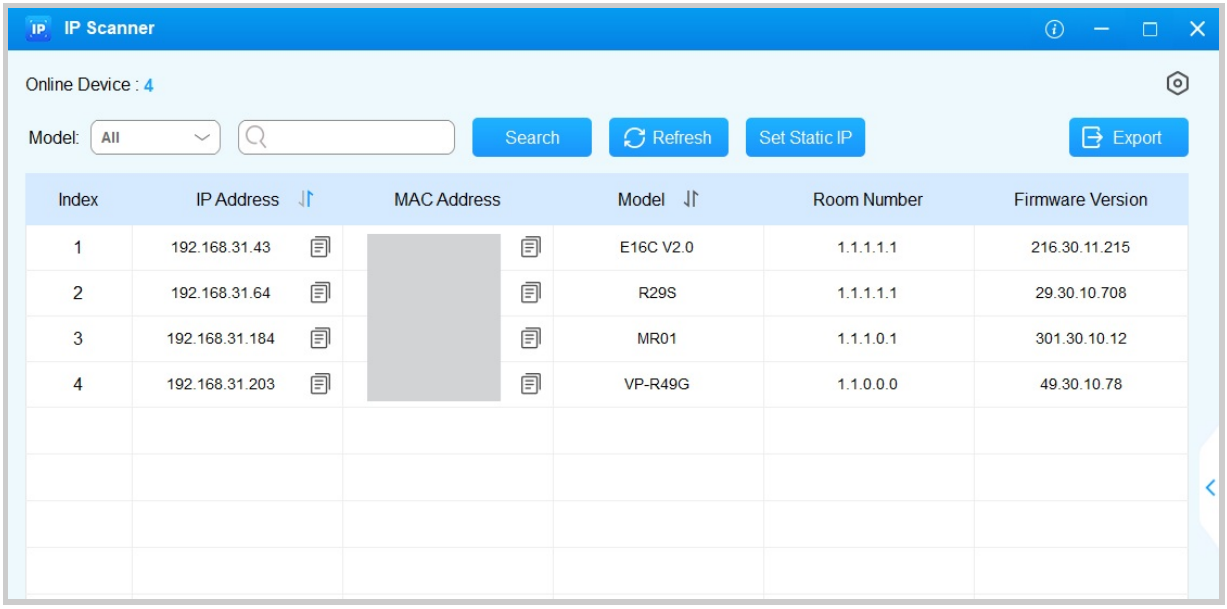
Access the Device

Obtain Device IP Address

Press the button on the top of the device and hold it until the device announces its IP.

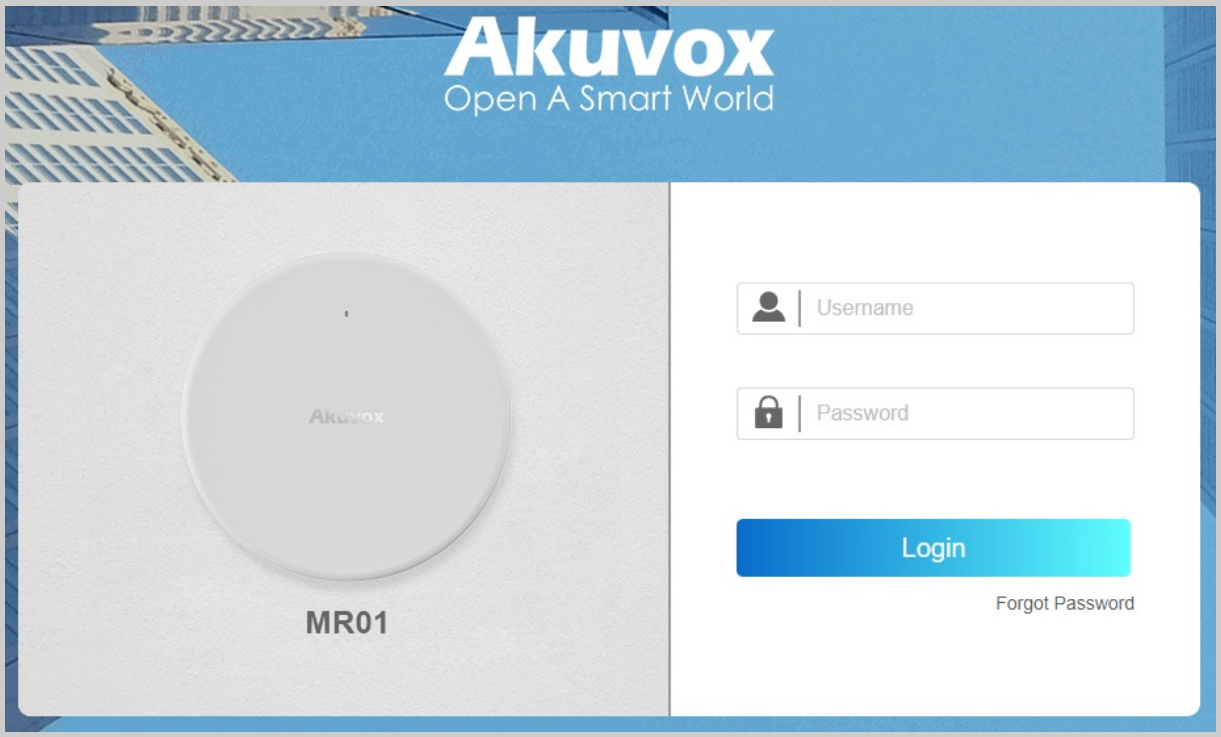


Or, scan the device IP with the **Akuvox IP Scanner Tool** on the same local network. Click **Refresh** to update the list.



Access the Device Settings

Enter the device IP address in a browser and log in to the device web interface, where you can configure and adjust parameters.



Note

- Download IP scanner: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- See the detailed guide: https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner
- Google Chrome browser is strongly recommended.
- The initial username and password are **admin,** and please be case-sensitive.

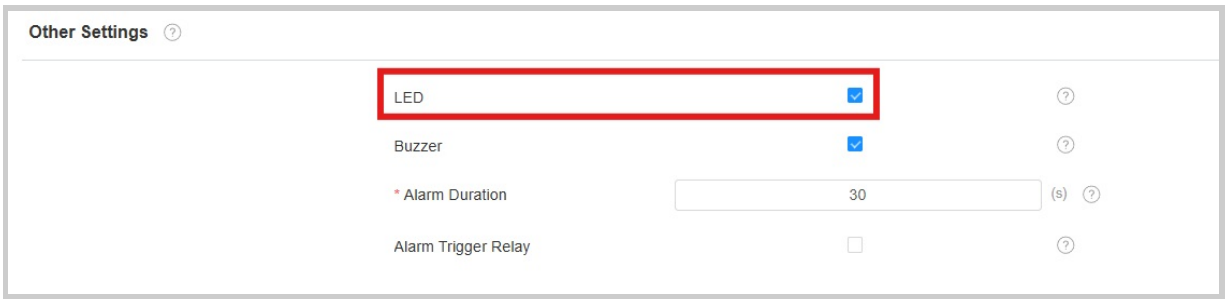
Indicator Light Status

The LED indicator shows the device status as described in the table below:

Status	LED Behavior
Normal operation (Ethernet connected, Wi-Fi connected, or hotspot enabled)	Green solid
Hotspot disabled and no Ethernet or Wi-Fi connection	Green slow flashing
Device resetting	Red flashing for 3 seconds, then the device reboots
Device starting up	Red solid (status updates after startup)
Device upgrading	Red solid (status updates after upgrade completes)
Network error	Green fast flashing
Fall detection verification	Red slow flashing
Fall alarm	Red fast flashing
Fall alarm triggered but not cleared (person not standing up, not returning to bed, and alarm not cleared manually)	Red fast flashing
Installation tilt warning (horizontal deviation greater than 15°)	Red fast flashing

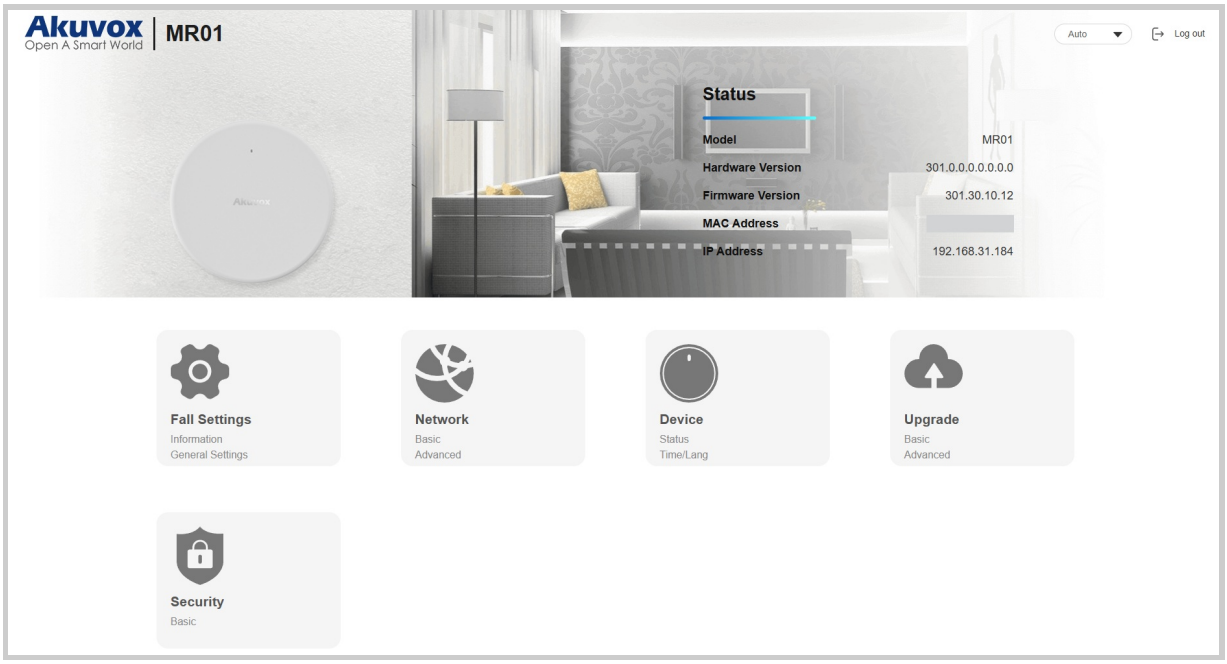
Turn on/off the LED

You can turn on/off the LED on the **Fall Settings > General Settings > Other Settings** interface.



Introduction to the Configuration Menu

- **Fall Settings**: This section is for configuring how the device detects falls and how fall alarms are triggered and reported.
- **Network**: This section mainly deals with DHCP & static IP settings, AP settings, device deployment, etc.
- **Device**: This section includes product and network information, and language and time settings.
- **Upgrade**: This section covers firmware upgrade, device reset & reboot, screenshots, configuration file auto-provisioning, PCAP, etc.
- **Security**: This section is for password modification, account status & session time-out configuration, and high-security mode.



Language and Time

Language

Select the device's web language in the upper-right corner.

The following languages are supported:

- English, Simplified Chinese, Traditional Chinese, Russian, Korean, Portuguese, Spanish, Dutch, French, German, Polish, Turkish, Japanese, Vietnamese, Italian, Arabic, and Bosnian.



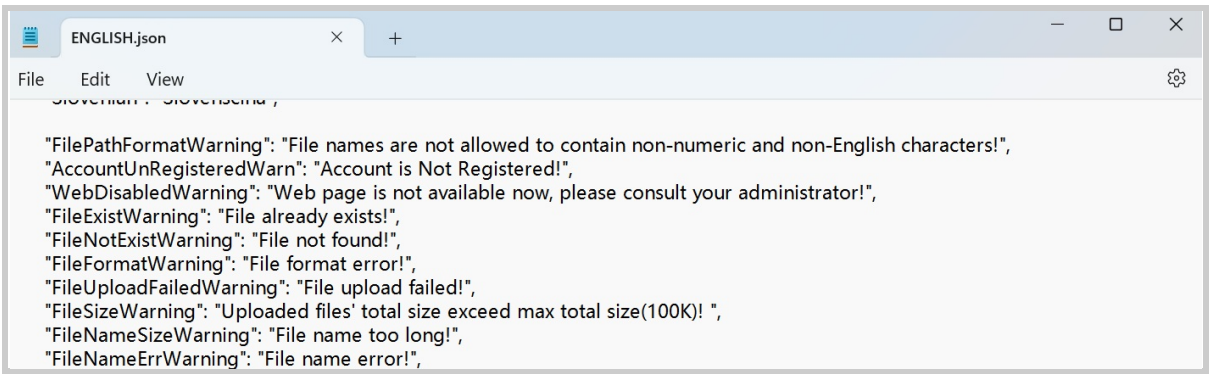
Custom Language

You can customize the configuration names and prompt texts on the web portal, such as the file name error warning.

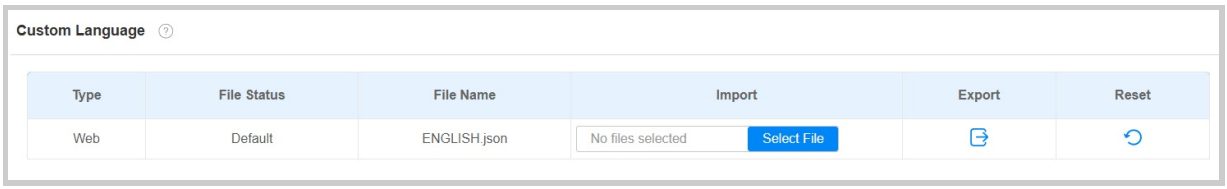
Export the .json file for editing. You may edit it with the notepad on your computer.

Import the .json file, and its size should be smaller than 1 MB.

File Example:



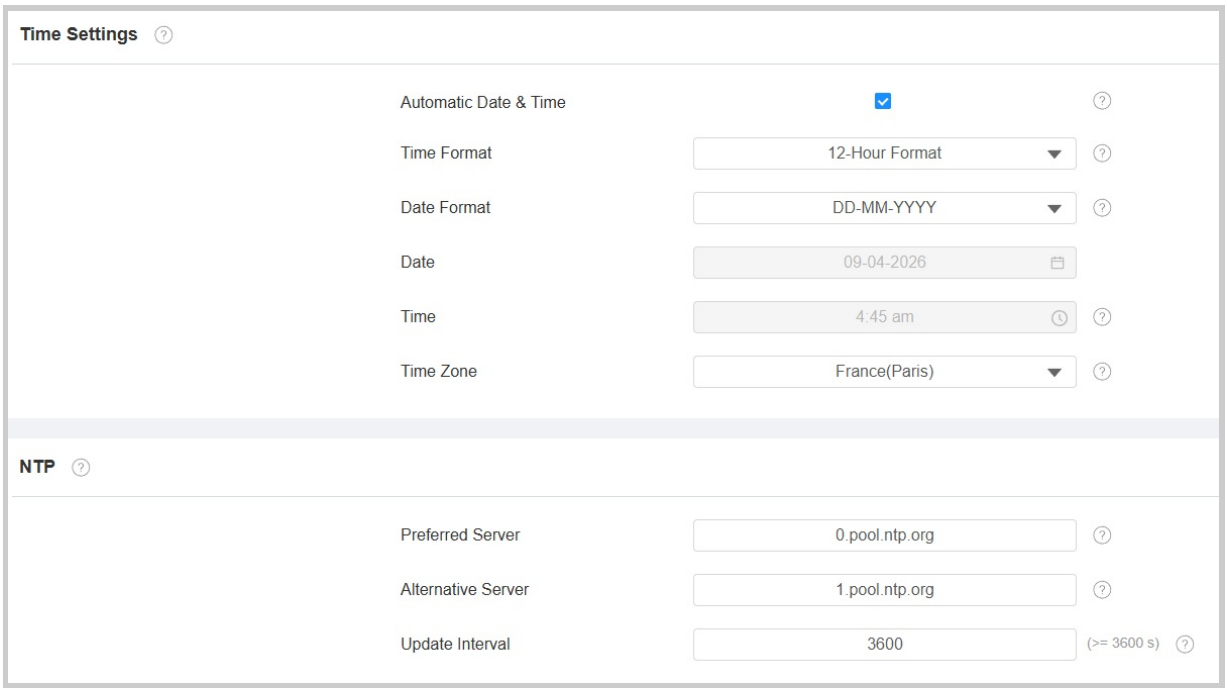
To set it up, navigate to **Device > Time/Lang > Custom Language** interface.



Time

The time settings on the web interface allow you to configure the NTP server address for automatic time and date synchronization. Once a time zone is selected, the device will notify the NTP server of the chosen time zone, enabling it to synchronize the time zone settings on your device.

Set it up on the **Device > Time/Lang** interface.

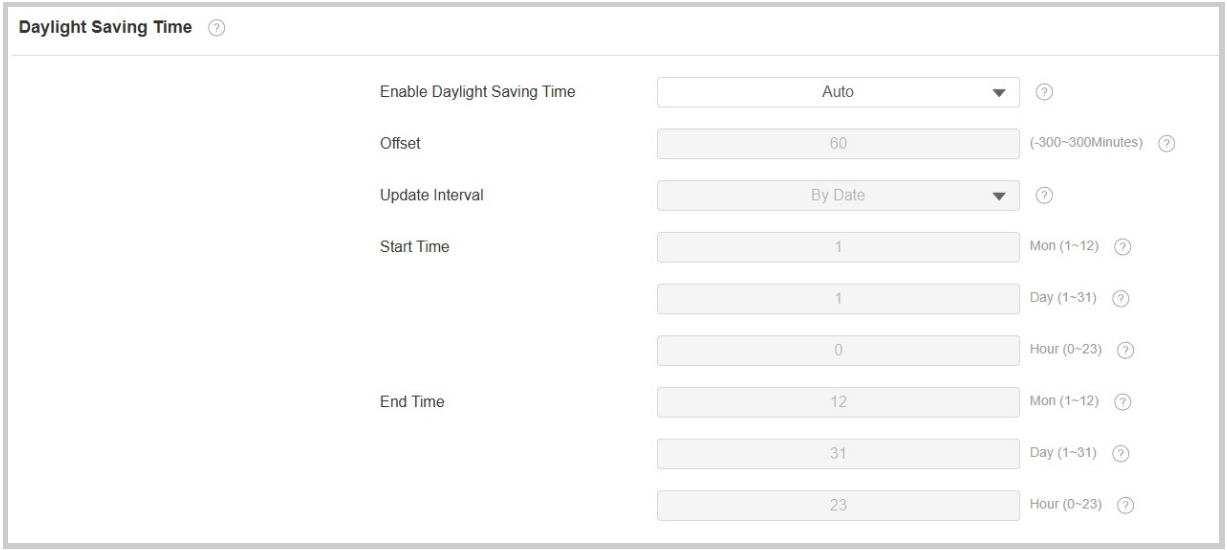


- **Automatic Date & Time**: The automatic date is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the Network Time Protocol(NTP) server. You can also set it up manually by switching it off and entering the time and date.
- **Time Format**: Select a 12-hour or 24-hour time format.
- **Date Format**: Select the date format from the available options.
- **Time Zone**: Select the specific time zone depending on where the device is used. The default time zone is GMT+0:00.
- **Preferred Server**: Enter the NTP server address.
- **Alternative Server**: Enter the backup server address. When the main NTP server fails, it will change to the backup server automatically.

Daylight Saving Time

Daylight Saving Time is the practice of advancing clocks (typically by one hour) during warmer months so that darkness falls at a later clock time. You can modify the time parameters to achieve longer evenings or daytime, especially in summer.

Set it up on the **Device > Time/Lang** interface.



- **Enable Daylight Saving Time**: Enable or disable the feature. **Auto** means that the device adjusts the daylight saving time automatically.
- **Offset**: 60 minutes as default, setting the clocks an hour ahead of the standard time.

- **By Date/By Week**: **By Date** sets the date schedule for daylight saving time. **By Week** sets the schedule for daylight saving time according to the week and month.

Network Setting

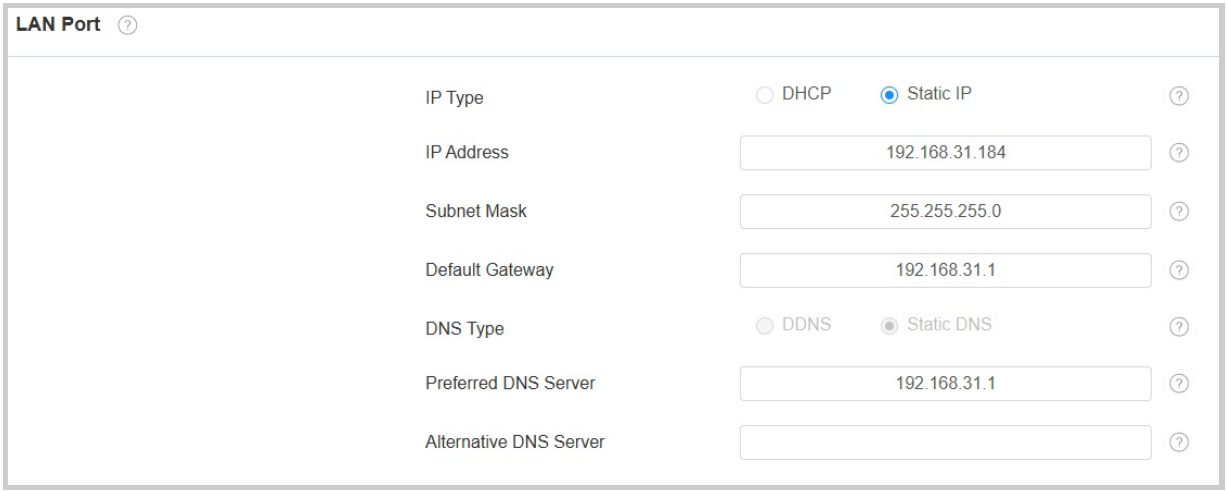
Check Network Information

Check the device network status on the **Device > Status** interface.

Device Network Configuration

To ensure normal functioning, make sure that the device has its IP address set correctly or obtained automatically from the DHCP server.

Set it up on the **Network > Basic** interface.



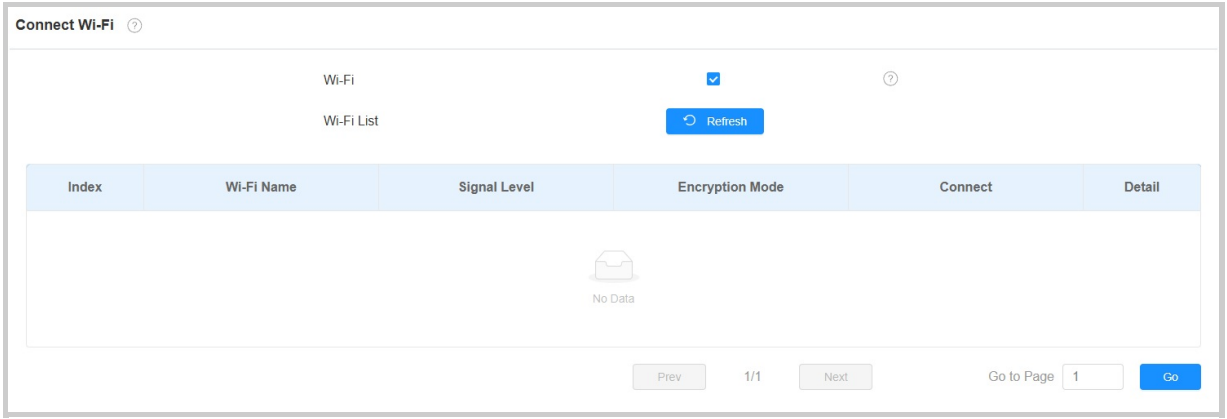
- **IP Type:** DHCP mode is the default network connection. The device will be assigned by the DHCP server with an IP address, subnet mask, default gateway, and DNS server address automatically. In static IP mode, the IP address, subnet mask, default gateway, and DNS server address have to be manually configured according to the actual network environment.
- **IP Address**: Set up the IP address when the static IP mode is selected. To access the device's web settings, your computer should be on the same local network as the device.

- **Subnet Mask**: A subnet mask tells your device which IP addresses are part of your local network and which ones are not. For example, if the subnet mask is 255.255.255.0, it means that devices with similar starting IPs (like 192.168.1.x) are in the same network.
- **Default Gateway**: The gateway is like a bridge between your device and other networks, such as the internet. Usually, it's the IP address of your router.
- **DNS Type**: Domain Name System(DNS) is the overall system or network that handles the translation of domain names (like www.example.com) into IP addresses (like 192.0.2.1), which computers use to identify each other on a network.
    - **DDNS**: Dynamic DNS. It is obtained automatically through the DHCP server.
    - **Static DNS**: When selected, you need to enter the DNS manually.
- **Preferred & Alternative DNS Server**: The preferred and alternative Domain Name Server(DNS). The device will connect to the backup server when the primary server is unavailable.

Wi-Fi Connection

Connect the device to a Wi-Fi on the **Network > Basic** interface.

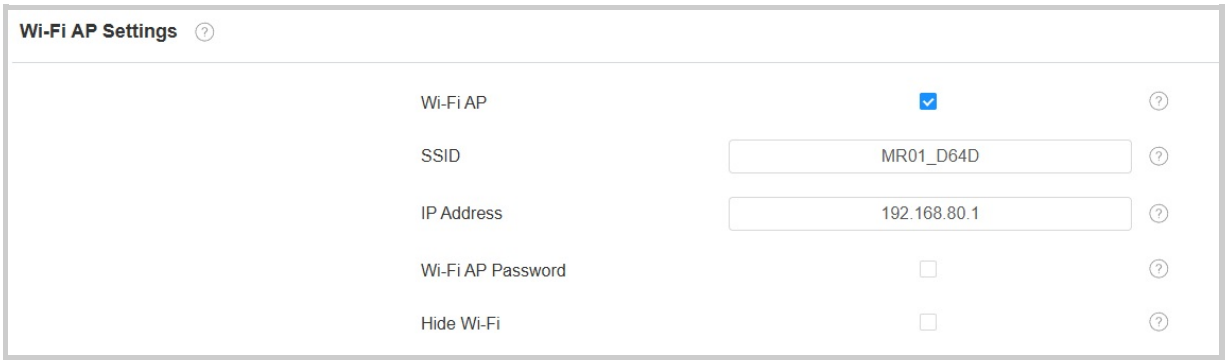
The available Wi-Fi will display after Wi-Fi connection is enabled. Connect to the desired Wi-Fi by clicking **Connect** and entering the password.



Wi-Fi AP Setting

The device supports AP mode, allowing it to function as a Wi-Fi hotspot for other devices to connect for configuration or network access.

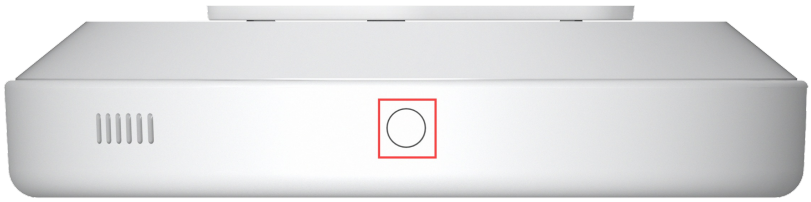
Set it up on the **Network > Basic** interface.



- **Wi-Fi AP**: Enable/disable the feature.
- **SSID**: The device's Wi-Fi name.
- **IP Address**: The management IP address of the device when AP mode is enabled. After connecting to the device Wi-Fi hotspot, enter this IP address in a web browser to access the configuration page.
- **Wi-Fi AP Password**: Set the Wi-Fi password if needed.
- **Hide Wi-Fi**: If enabled, this Wi-Fi will not be scanned by other devices.

You can also enable the device's AP mode by holding its physical button for 3 seconds.

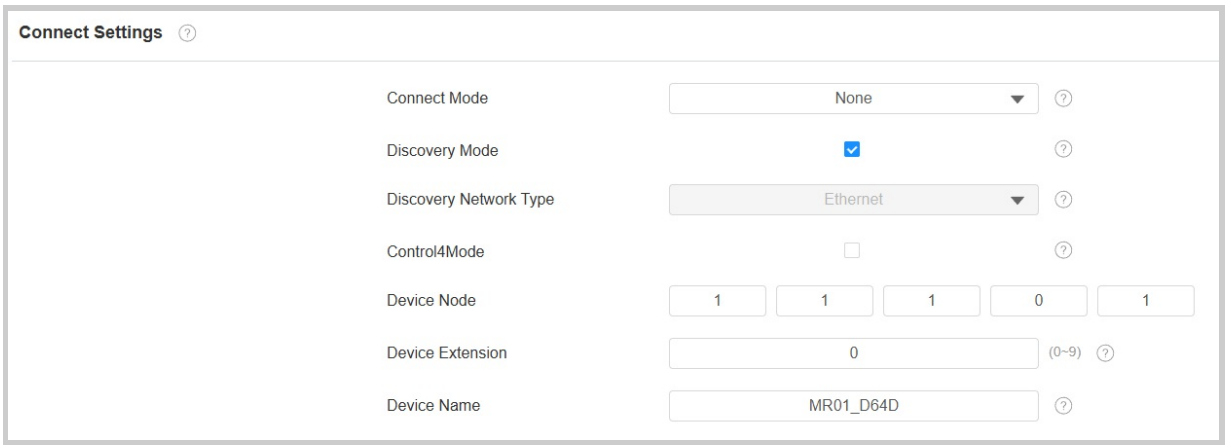
Holding it for 3 seconds again to turn the mode off.



Device Deployment in Network

To facilitate device control and management, configure Akuvox intercom devices with details such as location, operation mode, address, and extension numbers.

Deploy the device in the network on the web **Network > Advanced > Connect Setting** interface.



- **Connect Mode**: It is automatically set up according to the actual device connection with a specific server in the network, such as **SDMC**, **Cloud,** or **None**.

  - **None**: None is the default factory setting, indicating the device is not in any server type. Devices connect directly to each other or within a local area network (LAN) without relying on external servers.
  - **Cloud**: The device is connected to the SmartPlus Cloud, a cloud-based system simplifying property access management. The Cloud mode allows devices to interact intelligently with one another and the mobile SmartPlus App, backing up data daily and on different hosts. It suits projects requiring smart, flexible, and secure deployment and management.
  - **SDMC**: The device is connected to the SDMC, a management platform designed for on-premise projects. The SDMC mode manages and backs up data remotely on a local network. It also boasts many features suitable for projects requiring high privacy, lower cost, and centralized management.

- **Discovery Mode**: Enabled by default. Available for **None** server mode. The device can be discovered by other devices in the network. When disabled, the device will be concealed and not be discovered by other devices.
- **Device Network Type**: Specify the preferred network connection, WLAN or Ethernet. It is Ethernet by default. When Ethernet is unavailable, the device will automatically switch to a WLAN connection and vice versa.

- **Control4 Mode**: Enable this option for integration with the Control4 smart home.
- **Device Node**: Available for **None** server mode. Uneditable in Cloud and SDMC mode. It can be used to call the device. Specify the device address by entering device location information from left to right: Community, Building, Unit, Floor, and Room in sequence.
- **Device Extension**: Available for **None** server mode. Uneditable in Cloud and SDMC mode. The device extension number ranges from 0 to 10.
- **Device Location**: The location in which the device is installed and used. Available for **None** server mode. Uneditable in Cloud and SDMC mode.

Device Local RTP Configuration

Real-time Transport Protocol(**RTP**) lets devices stream audio and video data over a network in real time.

To use RTP, devices need a range of ports. A port is like a channel for data on a network. By setting up RTP ports on your device and router, you can avoid network interference and improve audio and video quality.

Set it up on the **Network > Advanced** interface.



- **Starting RTP Port**: Set the port value to establish the start point for the exclusive data transmission range.
- **Max RTP Port**: Set the port value to establish the endpoint for the exclusive data transmission range.

Device Web HTTP Setting

This function manages device website access. This device supports the HTTPS remote access method.

Set it up on the **Network > Advanced** interface.



- **HTTPS Port**: Specify the web server port for accessing the device web interface via HTTPS.

SNMP Setting

Simple Network Management Protocol**(SNMP)** is a protocol for managing IP network devices. It allows network administrators to monitor devices and receive alerts for attention-worthy conditions. SNMP provides variables describing system configuration, organized in hierarchies and described by Management Information Bases (MIBs).

Set it up on the **Network > Advanced** interface.



- **SNMP Port**: Set a specific port for the data transmission from 1024 to 65535.
- **Trusted IP**: Enter the third-party IP address.

Fall Setting

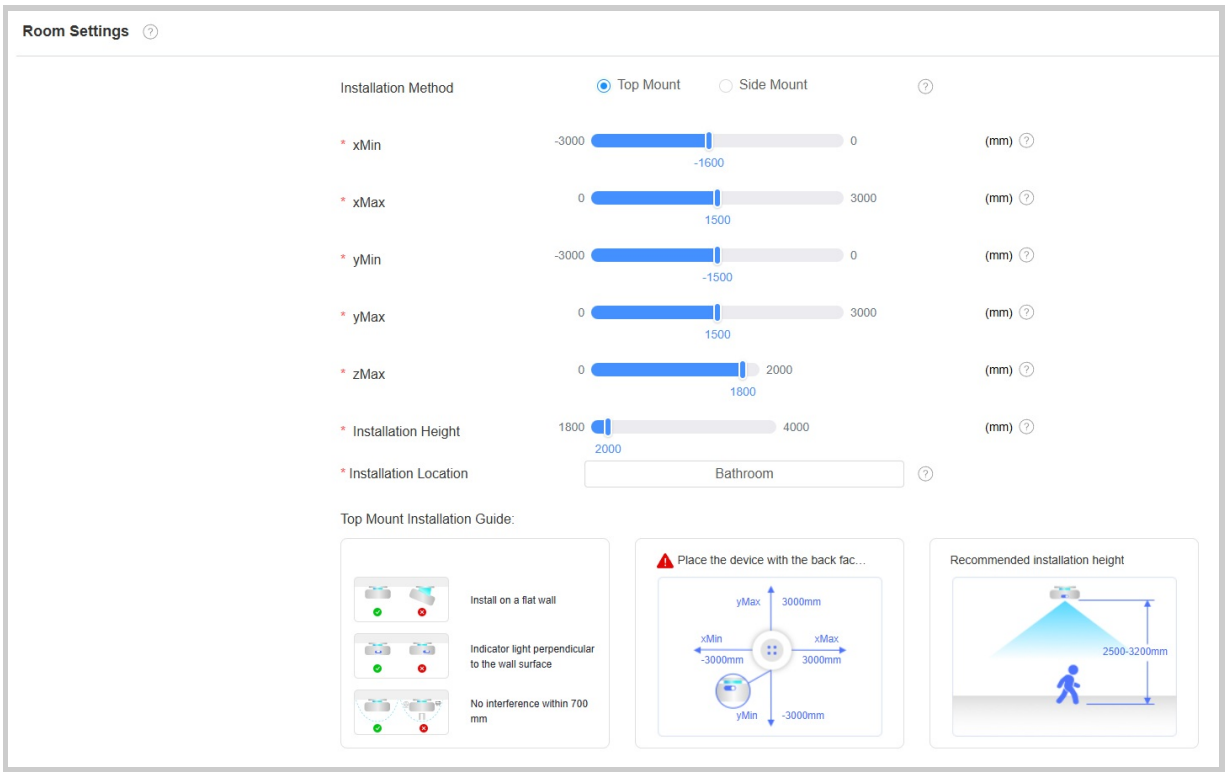
This chapter introduces the key functions used to configure and monitor fall detection within a room.

- **Room Space Definition**
  Defines the overall detection area of the MR01 using a coordinate system centered on the device. It determines the spatial range in which all detection activities take place.
- **Sub-region Configuration**
  Allows the room space to be divided into multiple functional areas (such as bed, door, or shielded zones), enabling different detection behaviors in different parts of the room.
- **Fall Detection**
  Detects when a person falls within the defined space or subregions, based on configurable time thresholds for confirmation and reporting.
- **Occupancy Detection**
  Identifies whether a person is present within a specific region, supporting real-time monitoring of room activity.
- **Bed-exit Detection**
  Monitors whether a person leaves the bed within a defined time period, typically used for nighttime or care scenarios.
- **Room Status Visualization**
  Provides a real-time view of the room, including personnel positions, detection results, and subregion statuses.

Room Setting

You can define the overall detection area and installation parameters of the device, which determine the spatial scope for all detection functions.

Set it up on the **Fall Settings > General Settings** interface.



- **Installation Method**: Specify how the device is mounted, which affects coordinate ranges and height constraints.
    - **Top Mount**: The device is mounted on the ceiling.
    - **Side Mount**: The device is mounted on a wall.
- **Coordinate System**: Define the reference coordinate system used to describe the detection space, with the device as the center point.
    - **xMin**: The minimum x-coordinate centered around MR01(-3000 to 0). The default value is -1500.
    - **xMax**: The maximum x-coordinate centered around MR01(0 to 3000). The default value is 1500.
    - **yMin**: The minimum y-coordinate centered around MR01. The default value is -1500.
        - When selecting top-mounted, the value range is from -3000 to 0.
        - When selecting side-mounted, the value range is from -5000 to 0.
    - **yMax**: The maximum y-coordinate centered around MR01(0 to 3000). The default value is 1500.
    - **zMax**: The height of the detection space. When top-mounted, the default value is 1800, and the value range is from 0 to 4000.

- **Installation Height**: The installation height of MR01.
    - When top-mounted, the installation height is the distance from the floor to the device plane. The default value is 2000, and the value range is from 1800 to 4000.
    - When side-mounted, the installation height is the distance from the floor to the center of the device. The default value is 2000, and the value range is from 1800 to 3200.
- **Installation Location**: The installation location of MR01.

Parameter Relationships

- xMin < xMax
- yMin < yMax
- Step size for all coordinates: 50 mm

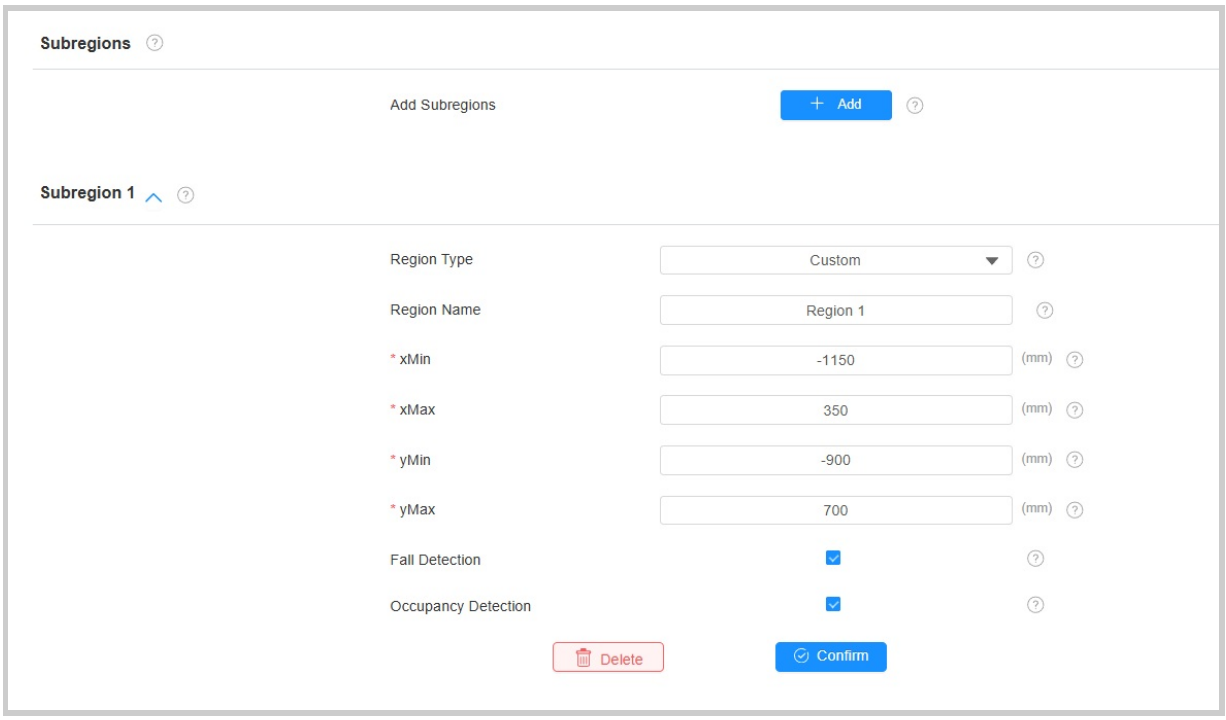
Height Rules:

- Top Mount: Installation Height ≥ zMax
- Side Mount: No restriction between Installation Height and zMax

Sub-region Setting

You can divide the room space into multiple functional regions to enable different detection behaviors within each area.

Add sub-regions on the **Fall Settings > Sub-regions** interface.



- **Add Sub-regions**: Click **+Add** to add a sub-region, and a default sub-region will be created on the spatial coordinate above.
    - You can adjust the size of the subregion by dragging the edges and vertices of the quadrilateral, and the corresponding coordinates will change accordingly.
    - A maximum of 6 subregions can be added.
    - By default, fall detection will be conducted in areas other than the subregions.
- **Region Type**: The default is **Custom**.
    - **Custom**: General-purpose region. Support fall & occupancy detection.
    - **Door**: Entrance area. Support fall & occupancy detection.
    - **Bed**: Bed area. Support bed-exit detection.
    - **Shield**: Excluded area. No fall detection.
- **Region Name**: Set the region name, which will display on the **Room Status** spatial coordinate.
- **Subregion Coordinates**: Specify the spatial boundaries of each subregion using the same coordinate system as the room.
    - **xMin**: The minimum x-coordinate of the subregion.
        - The default value is half of the minimum x-coordinate of the space, and the input range is integers from the minimum x-coordinate to the maximum x-coordinate of the space.

    - For example, if the minimum x-coordinate of the space is -1500 and the maximum x-coordinate is 1500, the default value will be -750, and the input range will be -1500 to 1500.
    - xMin must be less than xMax.
- **xMax**: The maximum x-coordinate of the subregion.
    - The default value is half of the maximum x-coordinate of the space, and the input range is integers from the minimum x-coordinate to the maximum x-coordinate of the space.
    - For example, if the minimum x-coordinate of the space is -1500 and the maximum x-coordinate is 1500, the default value will be 750, and the input range will be -1500 to 1500.
    - Max must be greater than xMin.
- **yMin**: The minimum y-coordinate of the subregion.
    - The default value is half of the minimum y-coordinate of the space, and the input range is integers from the minimum y-coordinate to the maximum y-coordinate of the space.
    - For example, if the minimum y-coordinate of the space is -2000 and the maximum y-coordinate is 2000, the default value will be -1000, and the input range will be -2000 to 2000.
    - yMin must be less than yMax.
- **yMax**: The maximum y-coordinate of the subregion.
    - The default value is half of the maximum y-coordinate of the space, and the input range is integers from the minimum y-coordinate to the maximum y-coordinate of the space.
    - For example, if the minimum y-coordinate of the space is -2000 and the maximum y-coordinate is 2000, the default value will be 1000, and the input range will be -2000 to 2000.
    - yMax must be greater than yMin.

- **Fall Detection**: Available when the **Custom** or **Door** region type is selected. Enabled by default, and falls will be detected within this subregion.

- **Occupancy Detection**: Available when **Custom, Door**, or **Shield** region type is selected. Enabled by default, and it detects whether there are individuals occupying this subregion.

When selecting the **Bed** region type, further configure the following options.

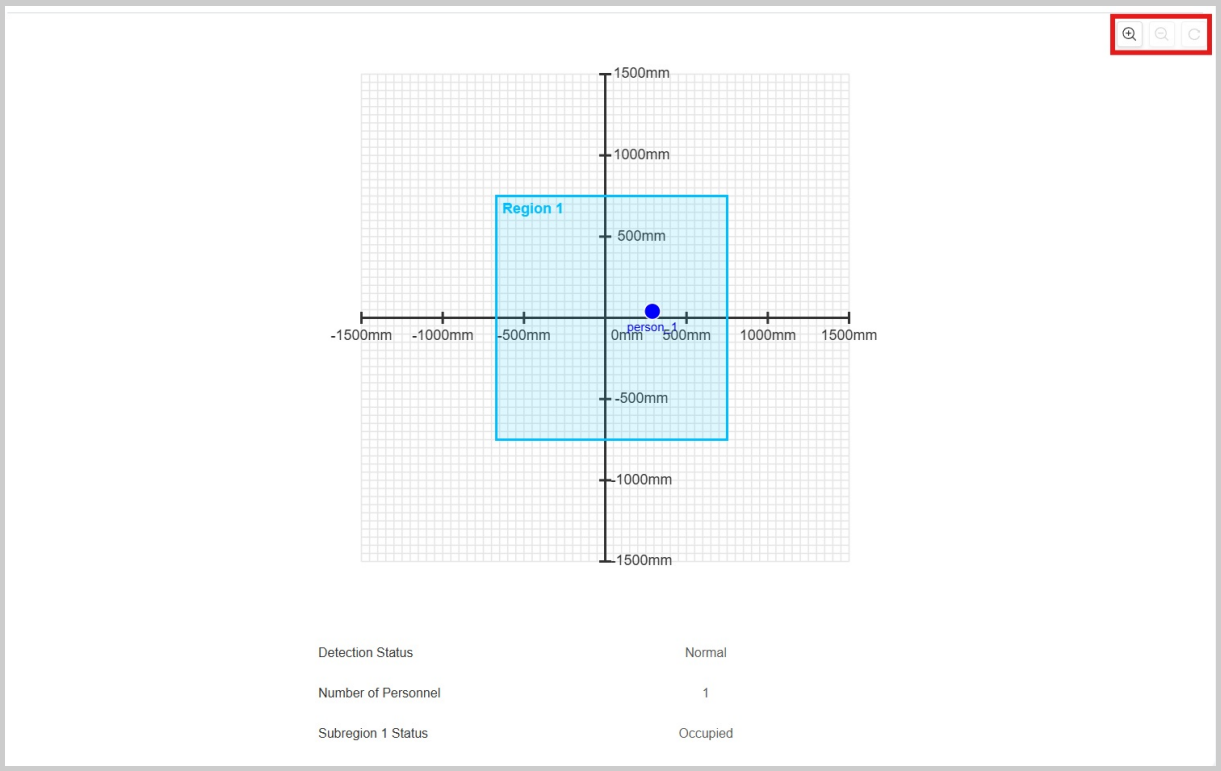
- **In-bed Detection**: An alarm will only be triggered if the individual leaves the bed 30 seconds after confirming they are in bed; if they return to the bed within 2 seconds, the bed-exit status will be cleared.
- **In-Bed Detection Start Time**: The start time for bed-exit detection.
- **In-Bed Detection End Time**: The end time for bed-exit detection.
- **Bed Height**: The bed height.
- **Bed-exit Time Threshold**: The time threshold for bed-exit detection. The default is 60 seconds; if the target leaves the bed for longer than the set time, an alarm will be triggered and reported. The input range is integers from 1 to 900 seconds.

Room Status

The **Room Status** section displays real-time detection results, including personnel status, region status, and system state.

The spatial coordinates show the size of the space based on the set XY coordinates, with the center being the installation position of MR01.

- You can click the **-** and **+** icons to zoom, and clicking the reset icon will restore the initial scale.
- You can move the view up, down, left, or right by holding the left mouse button.



- **Status of Individuals in the Space**:
  - Normal individuals: **Blue dots**.
  - If a fall or bed-exit alarm occurs, individuals in the space will be displayed as **red dots**.
  - The bed region will be highlighted **in red** during the bed-exit alarm.
- **Detection Status**: Display the current detection status of the space. The statuses include **Normal, Fall**, and **Bed-exit**.
- **Number of Personnel**: The number of individuals detected in the space.
- **Subregion x Status**: The status of the subregion. The statuses include **Normal, Fall, Bed-exit, Occupied**, and **Unoccupied**.

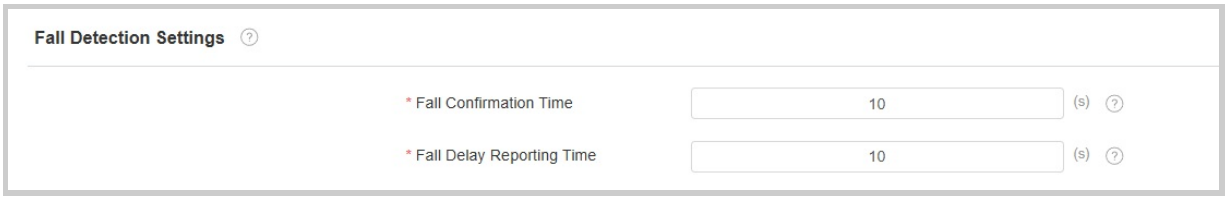
Note

- A subregion will display Occupied or Unoccupied only if **Occupancy Detection** is enabled.
- Subregion x will change according to the **Region Name** set for the subregion.
- A subregion will detect Fall and Bed-exit statuses only if **Fall Detection** and **In-bed Detection** are enabled.

Fall Detection Setting

You can configure the timing parameters used to confirm and report fall events.

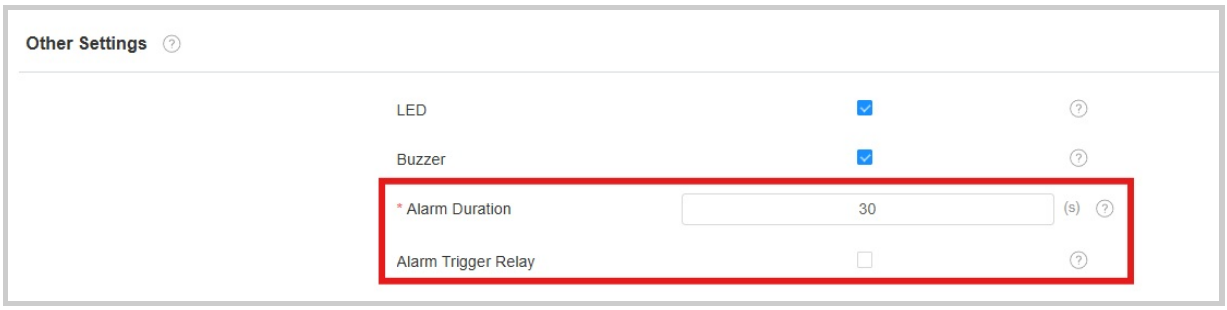
Set them up on the **Fall Settings > General Settings > Fall Detection Settings** interface.



- **Fall Confirmation Time**: The time threshold for confirming a fall. When the duration of the fall event reaches this value, it will be considered a fall event, triggering an alarm.
  The default value is 10 seconds, and the input range is from 0 to 30.
- **Fall Delay Reporting Time**: When the duration of the fall event reaches this value, it will be reported to the cloud, SDMC, indoor monitor, guard phone, or third-party system.
  The default value is 10 seconds, and the input range is from 0 to 30.

Alarm Setting

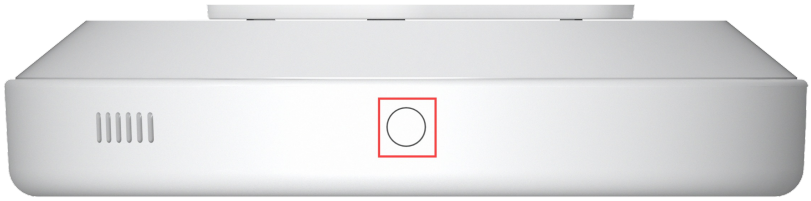
You can set the alarm duration and trigger relay on the **Fall Settings > General Settings > Other Settings** interface.



- **Alarm Duration**: The duration for which the alarm will sound(0 to 1800 seconds).
    - After reaching this time, the alarm sound will automatically stop, and it does not apply to the indicator light.
    - It is available only when the **Buzzer** is enabled.
    - The default value is 30 seconds.
- **Alarm Trigger Relay**: Determine whether to trigger the relay when an alarm occurs. This feature is off by default.
  When enabled, the relay will be automatically triggered when an alarm occurs.
- **Relay Hold Delay Time**: The duration for which the relay will hold after being triggered.
    - The default value is 3 seconds, meaning the relay will automatically turn off after 3 seconds.
    - The selectable range is from 1 to 60 seconds, or you can choose **Auto**.
      Auto indicates that the relay will automatically turn off only after the alarm is cleared locally (e.g., when a person stands up from the fall detection area, returns to bed, or when the device button/web page is used to clear the alarm).

Clear Alarm

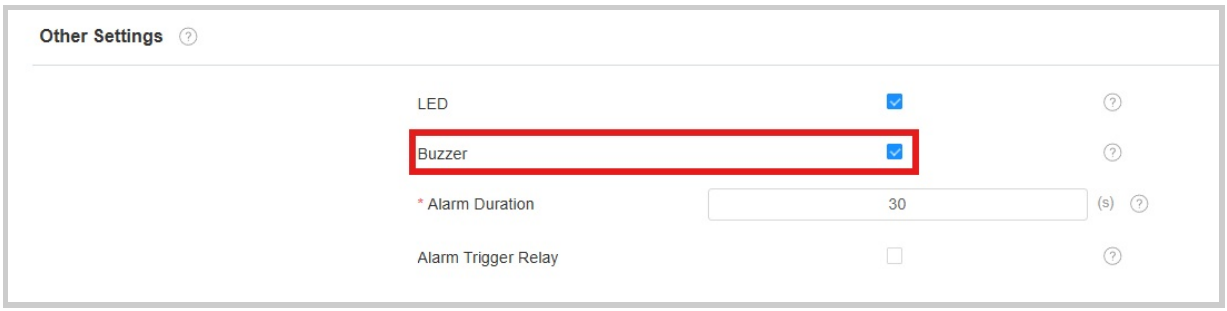
Clear the device alarm by short-pressing the physical button on its top.



Turn on/off Buzzer

You can turn on/off the buzzer on the **Fall Settings > General Settings > Other Settings** interface.

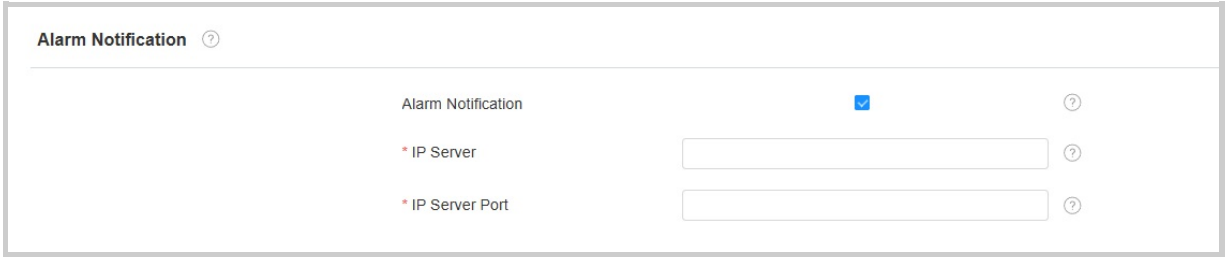
If disabled, the device will not sound an alarm.



Send Alarm Notification to Third-Party Server

The device can send detection records and alarm reports to third-party servers.

Set it up on the **Fall Settings > General Settings > Alarm Notification** interface.

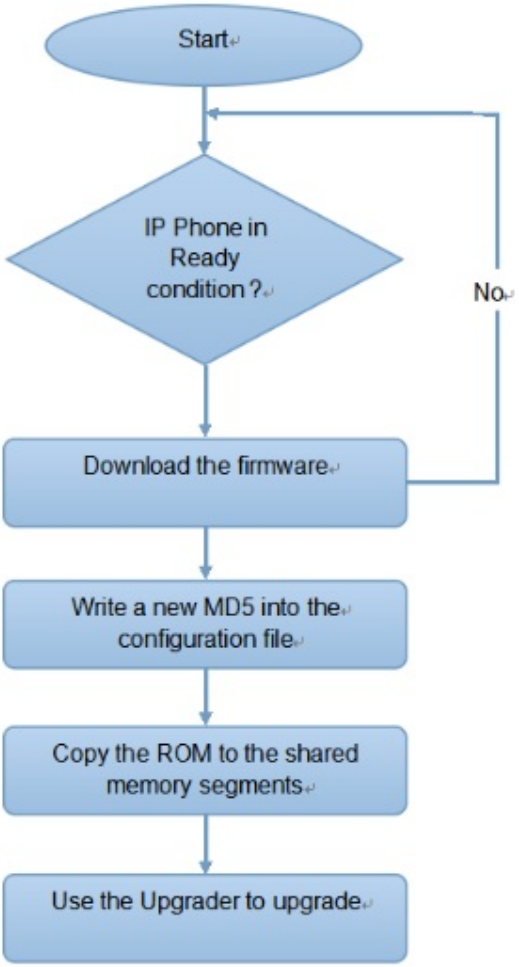


- **IP Server**: Enter the IP address of the third-party server.
- **IP Server Port**: Enter the port number for the third-party server.

Auto-provisioning

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:



Introduction to the Configuration Files

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

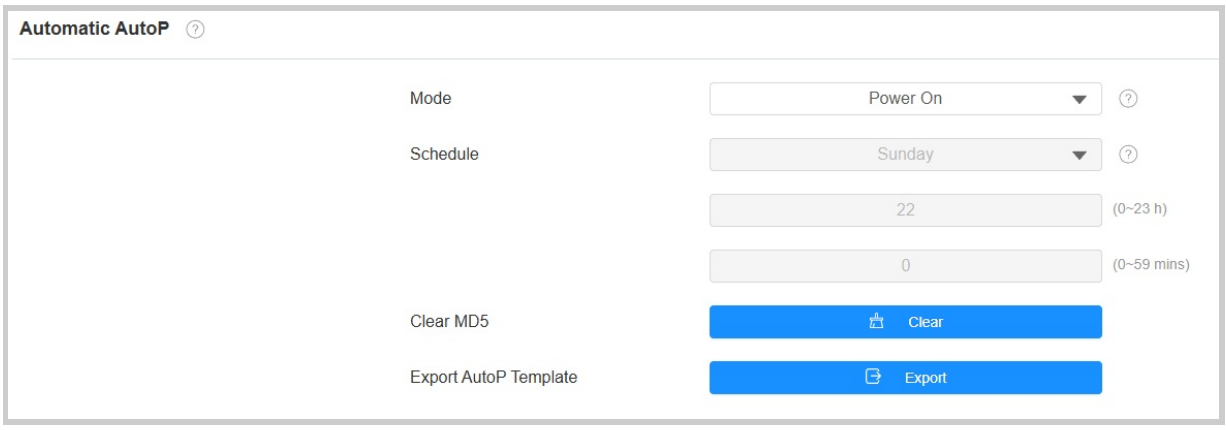
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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 up the schedule, go to the web **Upgrade > Advanced > Automatic AutoP** interface.

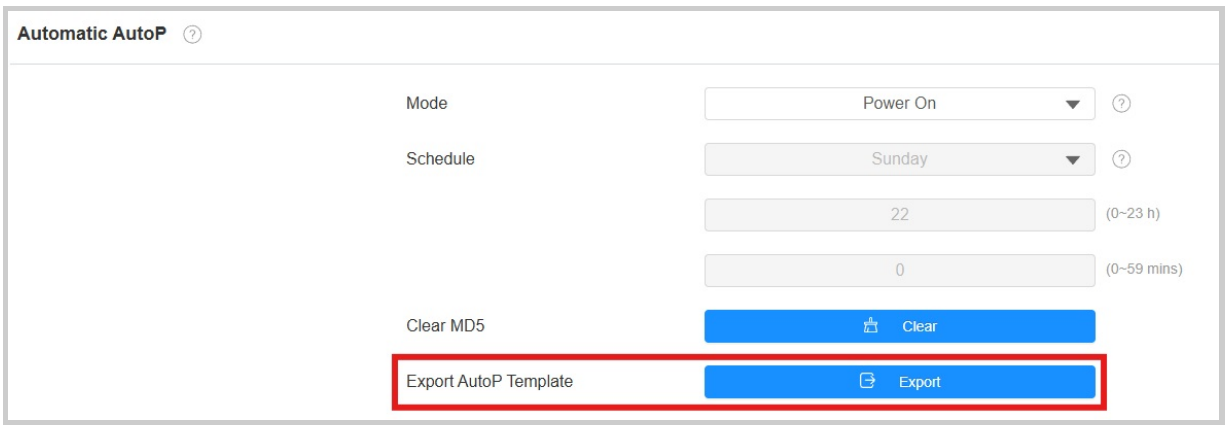


- **Mode**:
  - **Power On**: The device will perform Autop every time it boots up.
  - **Repeatedly**: The device will perform Autop according to the schedule you set up.
  - **Power On + Repeatedly**: Combine **Power On** mode and **Repeatedly** mode that will enable the device to perform Autop every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

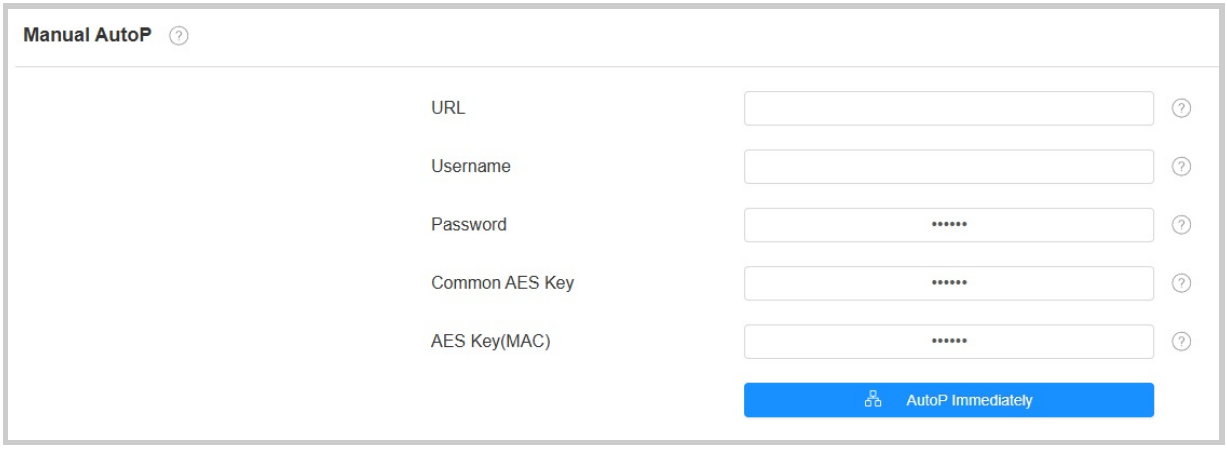
Static Provisioning Configuration

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 download the template, go to the **Upgrade > Advanced > Automatic AutoP** interface.



To set up the server, go to the **Upgrade > Advanced > Manual AutoP** interface.



- **URL**: Specify the TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **Username**: Enter the username if the server requires a username to be accessed.
- **Password**: Enter the password if the server requires 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

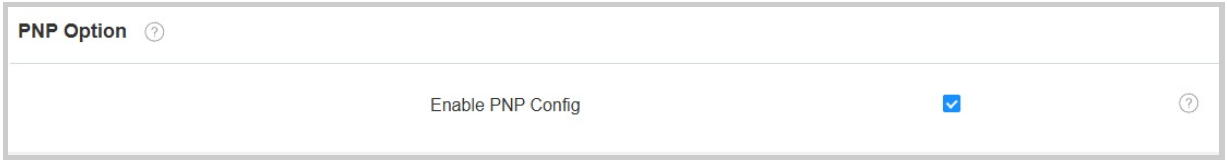
Akuvox does not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

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.

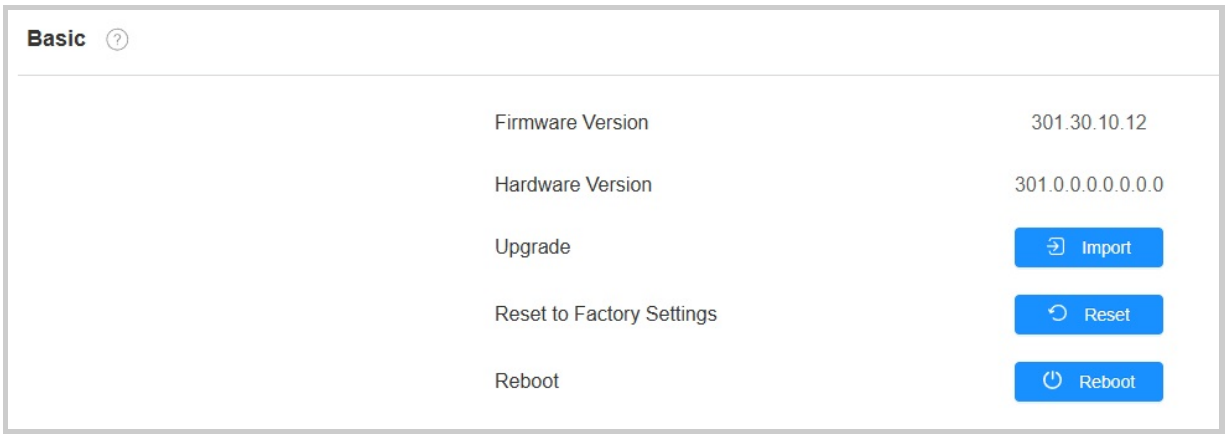
Click here to watch the configuration video.

To enable the function, go to the **Upgrade > Advanced > PNP Option** interface.



Firmware Upgrade

To upgrade the device, navigate to the **Upgrade > Basic** interface. Click **Import** to upload the firmware.



Note

Firmware files should be .rom format for an upgrade.

Security

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 the web **Security > Basic > Session Time Out** interface.



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.

To set it up, go to the web **Security > Basic > High Security Mode** interface.



Backup

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

To export the file, go to the **Upgrade > Advanced > Others** interface. The export file is in the TGZ file.

The import file should be in TGZ, CONF, or CFG format.

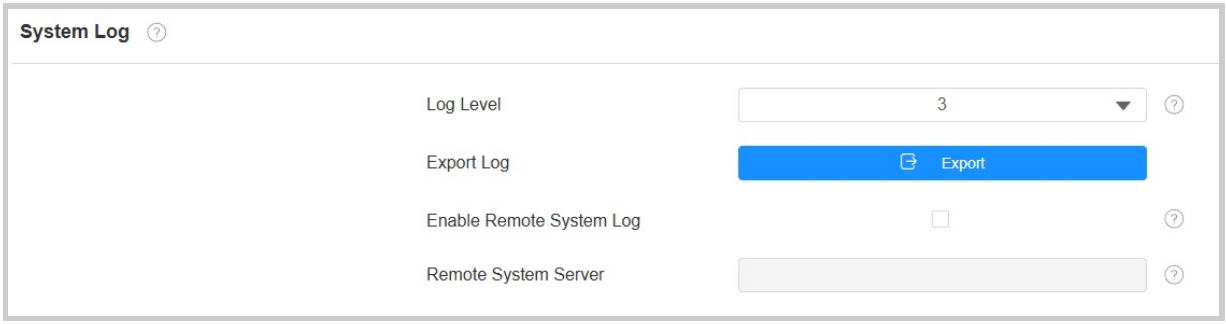


Debug

System Log for Debugging

System logs can be used for debugging purposes.

If you want to export the system log to a local PC or a remote server for debugging, you can set up the function on the web **Upgrade > Diagnosis > System Log** interface.

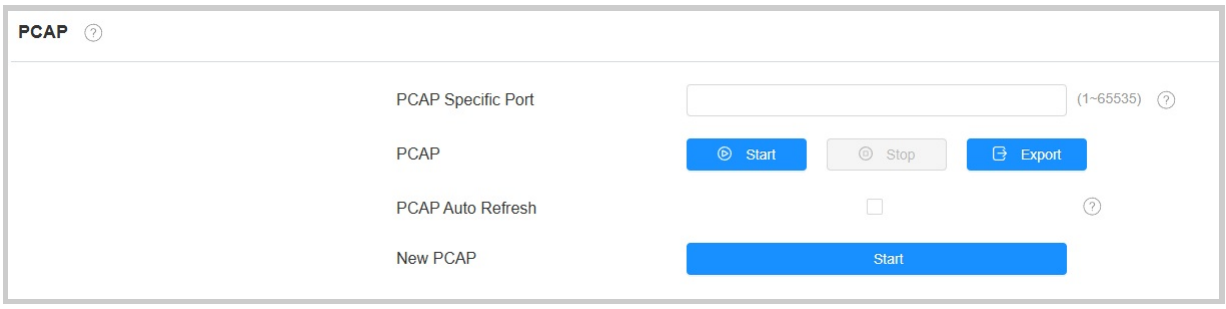


- **Log Level**: Log level ranges from 0 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log**: Click the **Export** tab to export a temporary debug log file to a local PC.
- **Remote System Server**: Enter the remote server address to receive the system log, and it will be provided by Akuvox technical support.

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 up PCAP, go to the web **Upgrade > Diagnosis > PCAP** interface.

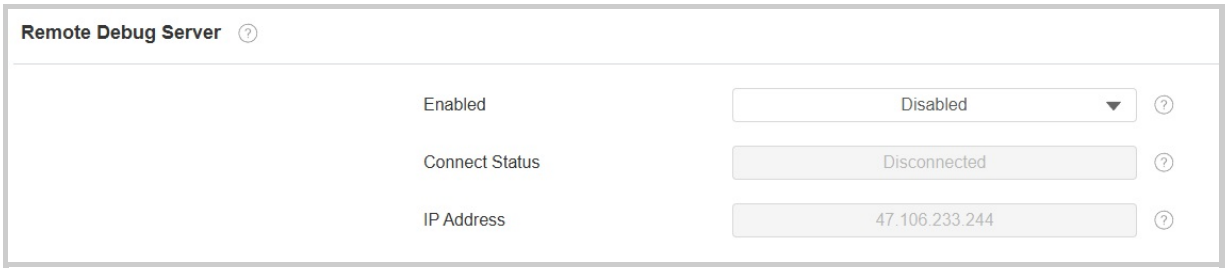


- **PCAP Specific Port**: Select the specific port from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP**: Click the **Start** tab and **Stop** tab to capture a certain range of data packets before clicking the **Export** tab to export the data packets to your Local PC.
- **PCAP Auto Refresh**: When enabled, the PCAP will continue to capture data packets even after the data packets reach 50M maximum in capacity. When disabled, the PCAP will stop data packet capturing when the data packets reach the maximum capturing capacity of 1MB.

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 **Upgrade > Diagnosis > Remote Debug Server** interface.



Point Cloud Data Export

You can export spatial detection data collected by the radar for technical analysis and troubleshooting purposes.

Export the data on the **Upgrade > Diagnosis > Point Cloud** interface. Click **Start** to start the data collection; click **Stop** to end the collection.


Point Cloud
Point Cloud
Start
Stop
Export

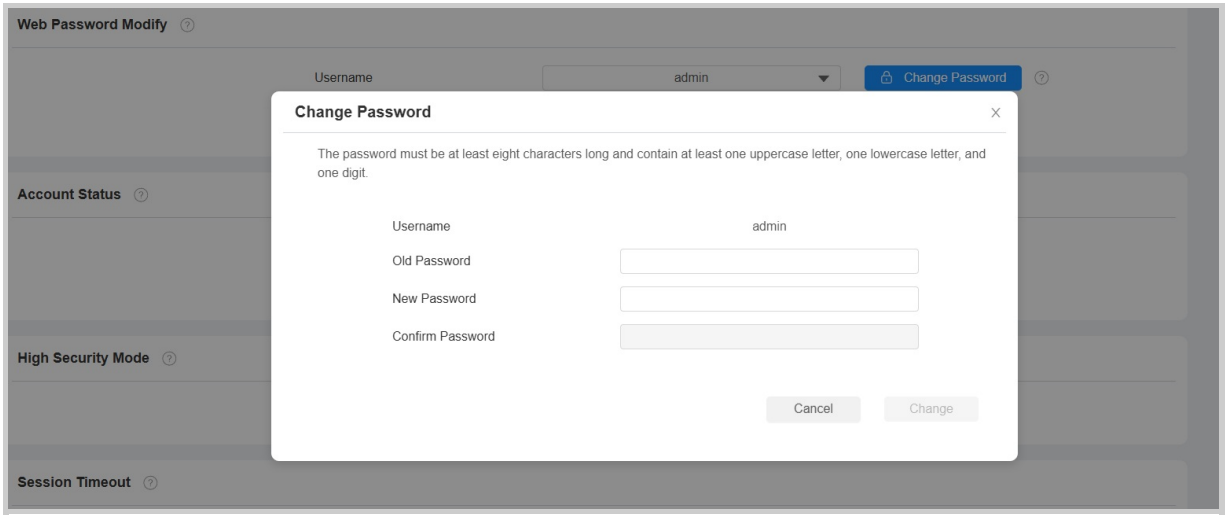
Password Modification

Modify Device Web Interface Password

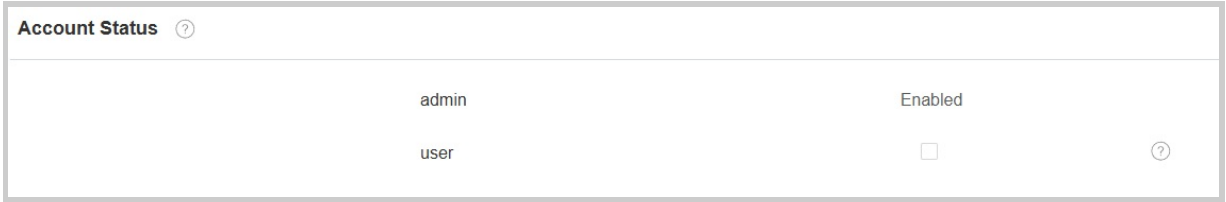
Select **Admin** for the administrator account and **User** for the user account. Click the **Change Password** tab to change the password.

To set it up, navigate to the **Security > Basic > Web Password Modify** interface.





You can enable or disable the user account on the **Security > Basic** interface.



Note

There are two accounts, one is admin; its password is **admin**. The other is user, and its password is **user**.

Modify Security Questions

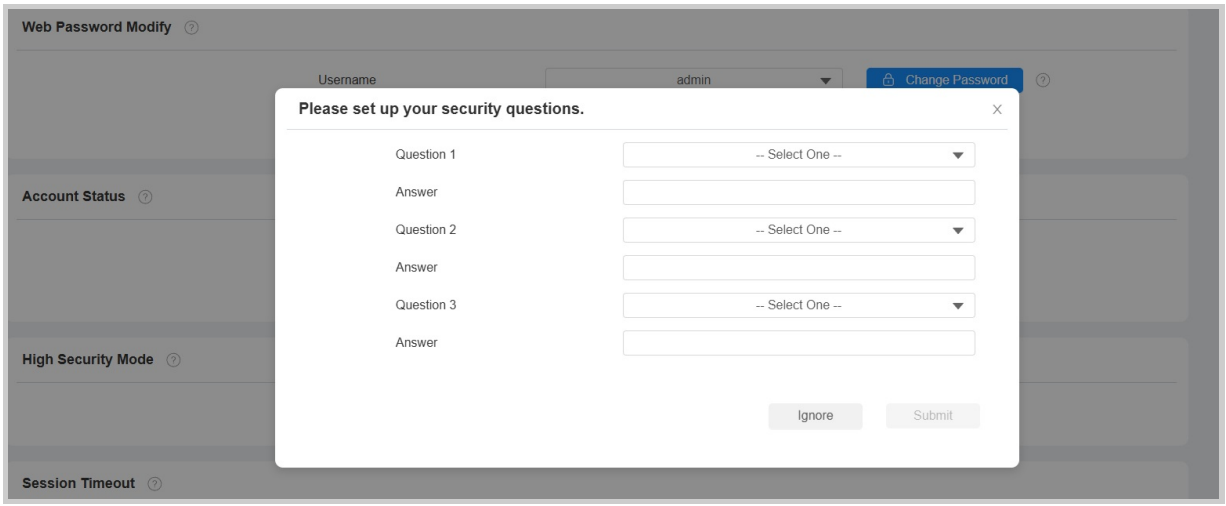
Security questions allow you to reset the web password if you forget it. After setting up the security questions, you can click "Forget Password" on the login interface, enter the answers, and a password reset window will pop up.

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

Set it up on the **Security > Basic > Web Password Modify** interface.



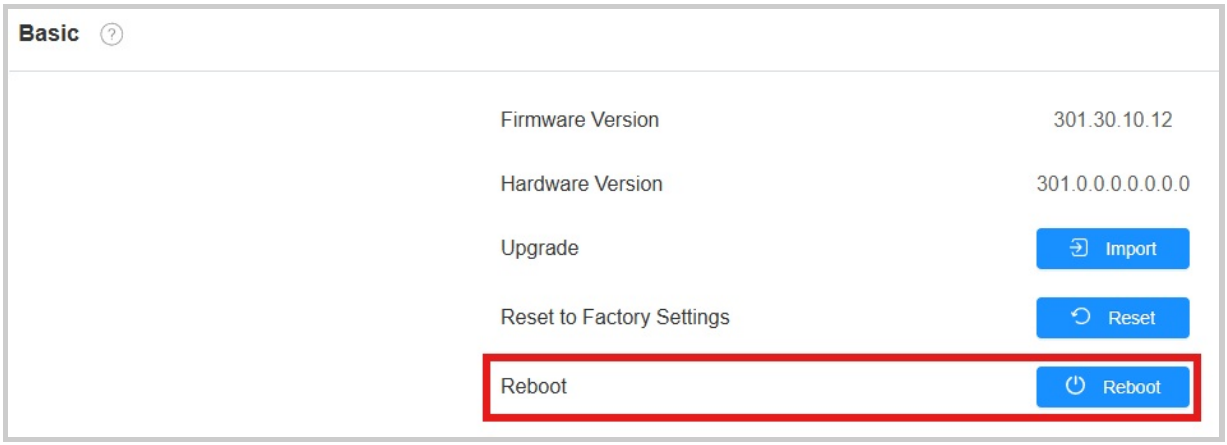
Enter the correct password for verification before setting up the security questions.



System Reboot & Reset

Reboot

Reboot the device on the **Upgrade > Basic** interface.



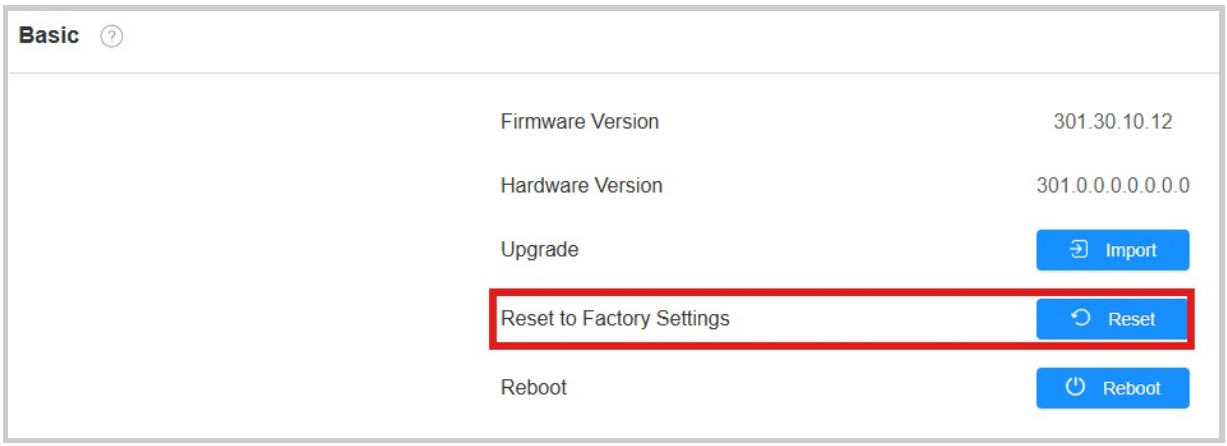
Besides, you can set up a reboot schedule to make the device restart at designated times.

Set it up on the **Upgrade > Advanced > Reboot Schedule** interface.



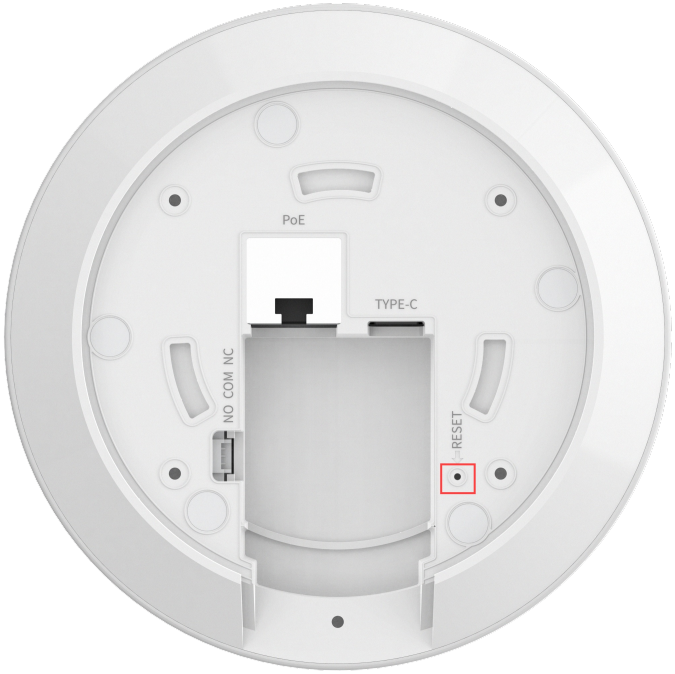
Reset

Reset the device on the **Upgrade > Basic** interface.



You can also reset the device by pressing the physical button.

1. Insert a PIN into the hole on the device's back.
2. Press and hold the button for about 3 seconds.
3. The indicator light flashes red slowly. Then, the device enters reset and reboot.



Powered by Document360