H501&H501W
User Manual

Version：V1.0 | Date：2025.2.24

Content

1 Safety Instruction

1.1 Safety Instruction

Please read the following safety notices before installing or using this unit. They are crucial for the safe and reliable operation of the device.

- Please use the product-specified power adapter. If you need to use a power adapter provided by another manufacturer due to special circumstances, please confirm that the voltage and current of the provided adapter meet the specifications of this product, and it is recommended to use a product that has passed safety certification, otherwise it may cause fire or electric shock accidents. When using this product, do not damage the power cord, do not twist, stretch and strap it, and do not press it under heavy objects or sandwich between items, otherwise it may cause fire or electric shock caused by broken power cord.
- Before using the product, please confirm that the temperature and humidity of the environment in which it is located meet the working needs of the product.
- Do not attempt to open it. Non-expert handling of the device could damage it. Consult your authorized dealer for help, or else it may cause fire, electric shock and breakdown.
- Please refrain from inserting metal objects such as pins or wires into the vents or crevices. Doing so may cause electric shock accidents due to the passage of current through the metal objects. If foreign objects or similar metallic items fall inside the product, usage should be stopped promptly.
- Please do not discard or store the plastic bags used for packaging in places accessible to children to prevent them from covering their heads, leading to obstruction of the nose and mouth, which may cause suffocation.
- Do not install this phone in an ill-ventilated place. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

2 Product Overview

2.1 Overview

The H501 & H501W series are compact, stylish, and cost-effective embedded intercom products. The H501W model features built-in 2.4G Wi-Fi 6, while both models support PoE power supply, making them ideal for indoor environments. Designed for seamless installation in standard 86-type boxes, they provide high-quality intercom communication. Perfect for residential communities and hotels, these devices enable voice communication with IP phones, improving service response times while enhancing the user experience and reducing operational costs.

2.2 Specification Parameter

Parameter	**H501**	**H501W**
2.4GHz Wi-Fi	/	Support
Wideband Coding	G.722, Opus	G.722, Opus
Network Speed	10/100 Mbps	10/100 Mbps
POE	Support	Support
Function Key	1	1
IP mode	IPv4/IPv6/IPv4&IPv6	IPv4/IPv6/IPv4&IPv6
Installation	86 box flush-mounted	86 box flush-mounted

3 Installation Instructions

3.1 Device Inventory

Device

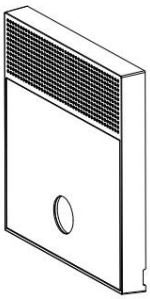
Connector*1

Quick Installation Guide

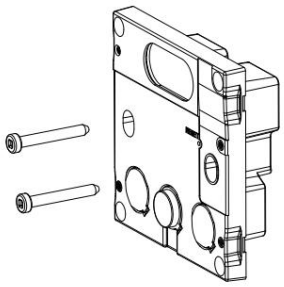
Screw * 2

3.2 Installation Procedure

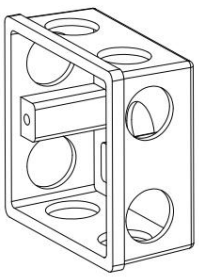
3.2.1 Stand Installation



Cover



Main body



86 Mounting box

1) First,remove the cover plate;

2) Connect the power cable and network cable, put the main body into the box 86. and use a screwdriver to screw in two PM4*30mm screws to fix the main body on the wall;

3) Check whether it works normally. The test method is as follows:

Press and hold the call button on the device for 3 seconds(30 seconds after the device is powered on). When the speaker makes a rapid beep sound, press Call button again quickly and the device automatically announces the IP address by voice. If the IP address works properly, continue with the following steps;

4) Cover the cover removed instep1;

3.2.2 Network Configuration Steps（H501W）

Method 1:

- Enter **[Advanced Settings]** on the W611W, then go to **[Share Wi-Fi]** to enable the Wi-Fi sharing function and set the office network SSID and password. At this point, the W611W functions as an AP.
- Power on the H501W devices.
- After powering up, the W611W will push the office network SSID and password to the H501W, enabling them to connect to the office network.

Method 2:

- The user creates a Wi-Fi network with the SSID "**WiFi-device-ssid**" and the password "**i<0%aY8+**".
- After powering on, the H501W devices will automatically connect to this Wi-Fi.
- The Wi-Fi information of the H501W can be modified through automatic deployment to connect to the office network.
- Wi-Fi module configuration file as shown:

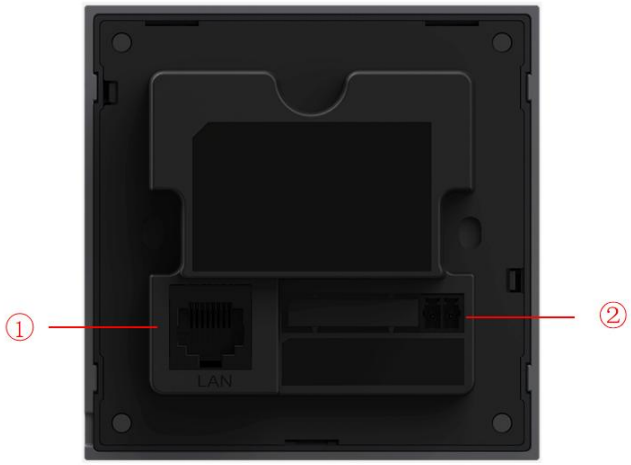
```
<<VOIP CONFIG FILE>>Version:2.0000000000

<NET CONFIG MODULE>

--WIFI List--     :
Item1 WIFI Name         :Redmi K60
Item1 WIFI SSID         :Redmi K60
Item1 Secure Mode       :1
Item1 WIFI Encryption   :1
Item1 WIFI User Name    :
Item1 WIFI Password     :12345678

<<END OF FILE>>
```

4 User Guide

4.1 Panel Description

Name	Instruction
Speaker	Play sound.
Call Button	By pressing the call button, you can call the set number.

4.2 Interface Specification



Serial Number	Interface	Instruction
①	Ethernet Interface	Ethernet interface：Standard RJ45 interface,10/100M auto-negotiation,it is recommended to use Category 5 or Category 5e Ethernet cable.
②	Power Interface	Power Interface: 12V/1A input

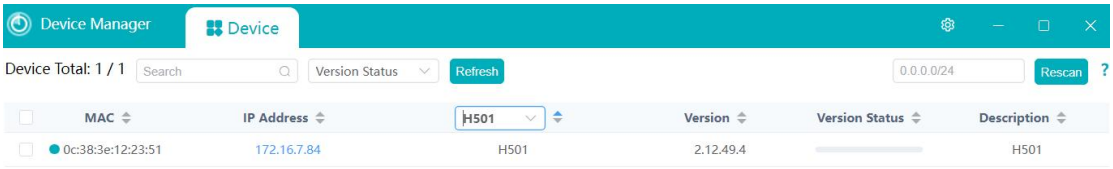
4.3 Web Management

4.3.1 Device IP Address

Retrieve Device IP through Scanning Tool:

1. The computer and device are connected to the same LAN, and Device Manager is installed on the PC.

2. Open the IP scanning tool (Device Manager), click on the scan button to obtain the IP address of the device within the local network.



Get the device IP through the device (the default is the English broadcast IP):

After the device has been completely started (it takes about 30 seconds approximately), in the standby mode, long-press the "Call Button" for 3 seconds. Once the speaker emits a prompt tone, release the button immediately. Then, quickly press the "Call Button" (the same button as the one for the long press mentioned above) within 5 seconds, and the device will start to announce the IP.

4.3.2 Web Interface

Ensure that the computer and the device are on the same local network. Open a web browser, enter the obtained device IP, log in to the device's web page, and access the login page.

Users must enter the correct username and password to log in to the web page. The default username and password are both "admin."

4.4 Device Status

Users can check the status of the device through the web page.

Log in to the web page, go to **[System] >> [Information]** page, and check the device status.

- System information: Displays device model name, hardware version number, software version number, running time, memory information, system time and other information.
- Network: Displays device network mode, MAC address, Ethernet IP, subnet mask, gateway and other information.
- Account: Displays the device registered account name/number, registration status and other information.

4.5 Language Settings

Users can set the language for through the web interface.

Set language in the web interface:

Log in to the device's web page, then set the language from the drop-down menu in the

top right corner of the page.When users check "Synchronic language to the phone," the webpage language will also synchronize the language on the LCD of the H6W phone.

4.6 Line Settings

The device supports two SIP accounts simultaneously, Users can switch between two SIP accounts as needed and register SIP accounts through the web interface.

Users can register a SIP account through the web page by navigating to **[Line] >> [SIP] >> [Line]**. selecting the registered line, and registering the SIP account through **[Register Settings]**. After completing the SIP parameter settings, click **[Apply]** to successfully register.

SIP Parameters:

Parameters	Description
Line Status	On this page, the current status of the line is displayed. To obtain the latest online status, users must manually refresh the page.
Activate	The status of this line is 'Activated'
Username	Enter the username of the service account.
Authentication User	Enter the authentication name of the service account.
Display Name	Enter the display name shown when a call request is sent.
Authentication Password	Enter the authentication password of the service account.
Server Address	Enter the SIP server address.
Server Port	Enter the SIP server port.

5 Call Features

5.1 Making Calls

When the user presses the "Call Button", the set number can be dialed out with just one click.

Configure Call Button on the web page:

Go to web, **[Function Key] >> [Function Key]**, type select **[Memory Key]**, enter the SIP account or IP address, subtype select **[Speed Dial]**. In standby mode, pressing this key directly initiates a quick call to the configured number.

5.2 Answer Call

5.2.1 Manually Answer

When there is an incoming call, the user can answer the call by pressing the "Call Button".

5.2.2 Auto Answer

Users can enable the auto-answer feature on the web page, allowing the phone to automatically answer incoming calls. Auto-answer can be enabled separately for each line. When disabled, the phone will ring upon an incoming call, and it won't automatically answer after a timeout.

Auto Answer Enabled For Line:

Log in to the device's web page, go to **[Line] >> [SIP] >> [Basic Settings]**, check **[Enable Auto Answering]**. After setting **[Auto Answering Delay]**, click **[Apply]**.

Auto Answer Enabled For IP Call:

Log in to the device's web page, go to **[Line] >> [Basic Settings] >> [SIP P2P Settings]**.

Check **[Enable Auto Answering]**, set the mode and auto-answer time, then click **[Apply]**.

5.3 End The Call

When on a call, press the "Call Button" to end the call.

6 Advance Function

6.1 MCAST

The MCAST function allows for easy and convenient broadcasting of announcements to every member of the multicast group. By setting the MCAST on the phone, multicast RTP streams can be sent to pre-configured multicast addresses. By configuring the listening multicast address on the phone, it can listen to and play RTP streams sent to that multicast address.

Users can configure the multicast listening address and port through the web page **[Device settings] >> [MCAST]**.

Configuration parameters:

Parameters	Description
SIP Priority	Defines the priority in the current call, with 1 being the highest priority and 10 the lowest.High-priority calls can be inserted into low-priority calls.
Intercom Priority	Defines the priority in the current call, with 1 being the highest priority and 10 the lowest.High-priority calls can be inserted into low-priority calls.
Enable Page Priority	Regardless of which of the two multicast groups is called in first, the device will receive the higher priority multicast first.
Enable Prio Chan	When enabled, the same port and channel can only be connected. Channel 24 is the priority channel, higher than 1-23; channel 0 means not to use the channel.
Mcast Listening Renew Time	After the device manually ends the multicast, it can automatically resume the multicast playback within the set timeout period.
Enable Emer Chan	When enabled, channel 25 has the highest priority.
Name	Set the multicast name.
Host:port	Set the multicast server address and port.
Channel	0-25 (24: Priority Channel, 25: Emergency Channel).

MCAST Dynamic：

Send multicast configuration information through **SIP Notify** signaling. After receiving the message, the device configures it to the system for multicast monitoring or cancels multicast monitoring in the system.

6.2 Hotspot

SIP hotspot is a simple utility. Its configuration is simple, which can realize the function of group vibration and expand the quantity of sip account.

Take one device A as the SIP hotspot and the other devices (B, C) as the SIP hotspot client. When someone calls device A, devices A, B, and C will ring, and if any of them answer, the other devices will stop ringing and not be able to answer at the same time. When A B or C device is called out, it is called out with A SIP number registered with device A.

Users can set up a SIP Hotspot on the web page of **[Line] >> [SIP Hotspot]**.

Configuration parameters:

Parameters	Description
Enable Hotspot	Enable or disable hotspot
Mode	Selecting 'SIP Hotspot' indicates that this device exists as a SIP Hotspot. Selecting 'Client' indicates that this device exists as a client."
Monitor Type	The monitoring type can be broadcast or multicast. If you want to restrict broadcast packets in the network, you can choose multicast. The type of monitoring on the server side and the client side must be the same, for example, when the device on the client side is selected for multicast, the device on the SIP hotspot server side must also be set for multicast.
Monitor Address	The multicast address used by the client and server when the monitoring type is multicast. If broadcasting is used, this address does not need to be configured, and the system will communicate by default using the broadcast address of the device's wan port IP.
Local Port	Fill in a custom hotspot communication port. The server and client ports need to be consistent.
Name	Fill in the name of the SIP hotspot. This configuration is used to identify different hotspots on the network to avoid connection conflicts.

Line Settings	Sets whether to enable the SIP hotspot function on the corresponding SIP line.

Client Settings:

As a SIP hotspot client, there is no need to set up a SIP account, which is automatically acquired and configured when the device is enabled. Just change the mode to "client" and the other options are set in the same way as the hotspot.

The device is the hotspot server, and the default extension is 0. The device ACTS as a client, and the extension number is increased from 1 (the extension number can be viewed through the **[SIP hotspot]** page of the webpage).

Calling internal extension:

- The hotspot server and client can dial each other through the extension number before.
- Extension 1 dials extension 0.

7 Device Settings

7.1 Time Plan

The Time Plan feature allows users to set specific actions to occur at either a particular time or within a period. A time point triggers an action at a specific moment, while a period triggers an action during a specified duration.

Users can access this functionality through the web page under **[Device Settings] >> [Time Plan]**. They can define a Name, Type, Repetition Period, along with the effective date and time, then click 'Add'. Once configured, the device will execute the designated action at the specified times.

Parameter description:

Parameters	Description
Time Plan Settings	
Enable Time Plan List	Enable the Time Management List. After it is enabled, the set action will be executed during the set time period.
Enable Time Plan Pause	Enable the Pause List. After it is enabled, the device will not execute the set actions during the set pause time period.
Time Plan	
Name	Enter a defined action name
Type	Timed reboot、Timed upgrade、Timed echo test、Timed play audio、Timed config
Repetition Period	No Repetition : execute once within the set time range Daily: Perform this operation in the same time frame every day Weekly: Do this in the time frame of the day of the week Monthly: the time frame of the month to perform this operation
Start Date	Effective Date
End Date	End Date
Effective Time	Set the time period for execution
Time Plan Pause	

Name	Enter a defined action name
Start Time	Start Time
Stop Time	Stop Time

Note:

If there's an ongoing call within the set time frame, skip and do not execute the restart or upgrade operation.

7.2 Action Plan

Action Plan application: a technical implementation defined and designed by Fanvil for remote control and behavior linkage between Fanvil terminal equipment and other equipment. That is, when an event occurson the Fanvil terminal, the terminal can perform an action, and this action is completed according to a Plan rule.

Setting method:

Users can visit the website **[Line] >> [Action Plan]** to configure action plan rules. After the setting is complete, the configuration is assigned to the corresponding device and updated, and the corresponding terminal will perform the corresponding action when the event occurs.

Parameter description:

Parameter	Description
Action	Action when the number configuration rule is triggered. Supported types are: MCAST: When a rule is triggered, the IP phone will convert the incoming call or multicast into multicast and send it to the configured multicast address and port.
Number	The dialing number corresponding to each Action Plan; supports the same number expression as the Dial Plan.
Type	Types of Time Periods When Rules are Triggered, including:

	Early: trigger execution before call establishment. Connected: trigger execution after call establishment.
Line	The selected rule corresponds to the matching SIP line.
Direction	Corresponding Handling Methods for Configured Rules: Both: Triggered for both inbound and outbound calls; Outgoing call: Triggered for outbound calls; Incoming call: Triggered for inbound calls.

7.3 Maintenance

7.3.1 Configurations

Users with administrator privileges can view, export, or import the phone configuration, or restore the phone to factory Settings.

- **Export Configurations**

  Right click to select target save as, that is, to download the device's configuration file, suffix ".txt", ".xml" (**Note: profile export requires administrator privileges**).

- **Import Configurations**

  Import the configuration file of Settings.

- **Clear Configuration**

  Select the modules to be cleared in the configuration file.

  SIP: Account-related configurations

  AUTOPROVISION: Automatic upgrade-related configurations

  TR069: TR069-related configurations

  MMI: MMI module, including authenticated user information, web access protocol, etc.

  DSSkey: DSSkey configurations

  Basic Network: Basic network settings

- **Clear User Data**

  Select the local data tables to be cleared, default is all selected.

- **Reset Device**

  All device data will be cleared, including configurations and database tables.

7.3.2 Upgrade

7.3.2.1 Web Page Upgrade

Upgrade the device software version by upgrading to the new version through the web page. Once the upgrade is completed, the device will automatically restart and update to the new version.

[System] >> [Upgrade] >> [Software Upgrade], select the file, choose the version, then click "**upgrade**".

7.3.2.2 Online Upgrade

Through online upgrading, devices can be upgraded.

Configuration for online upgrade by the administrator on the web page:

- Access the web page **[System]>>[Upgrade]>>[Upgrade Server]**, configure the upgrade server, and the update cycle, etc. Place the upgrade TXT file and software on the corresponding server. When the device detects that the software version number on the server is different from its own software version number, it will prompt for an upgrade.

Configuration parameter description:

Parameter	Description
Upgrade Server	
Enable Auto Upgrade	Check enable automatic upgrade, and the device can detect the txt version information and available versions in the HTTP server.
Upgrade Server Address1	Fill in the available primary upgrade server (HTTP server) address.
Upgrade Server Address2	Fill in the address of the available backup upgrade server

	(HTTP server). When the primary server is unavailable, request the backup server.
Upgrade Interval	The web page starts to automatically detect the upgrade and configure the interval. If the server has a new version, the device will prompt for the upgrade at the interval.
Software Upgrade	
Current Software Version	Displays the current device software version number.
Server software version	Displays the server software version number.
[Upgrade] button	When there is a corresponding TXT file and version on the server side, the **[Upgrade]** button changes from grayed out to available. Click **[Upgrade]** to choose whether to upgrade.
New version description	When the server has the corresponding TXT file and version, the and version information in txt will be displayed under the new version description information.

7.3.3 Auto Provision

Web page: go to **[System]>>[Auto Provision]**.

Devices support SIP PnP, DHCP options, Static provision, TR069. If all of the 4 methods are enabled, the priority from high to low as below:

PNP>DHCP>TR069> Static Provisioning

Transferring protocol: FTP, TFTP, HTTP, HTTPS

Parameter	Description
Basic Settings	
CPE Serial Number	Display the device SN.
Authentication Name	Configure the user name of FTP server; TFTP protocol does not need to be configured; if you use FTP protocol to download, if you do not fill in here, the default user of FTP is anonymous.

Authentication Password	Configure the password corresponding to the FTP server user.
Configuration File Encryption Key	If the device configuration file is encrypted , user should add the encryption key here.
General Configuration File Encryption Key	If the common configuration file is encrypted, user should add the encryption key here.
Download Fail Check Times	The default value is 1. If the download of the configuration fails, it will be re-downloaded 1 time.
Save Auto Provision Information	Configure whether to save the automatic update information.
Download CommonConfig enabled	Whether phone will download the common configuration file.
Enable Server Digest	If the terminal matches the configuration file content through Digest verification, then whenever the configuration on the server is modified, or if the configuration on the terminal does not match the one on the server, the terminal will also initiate an update download.
Provision Config Priority	It supports normal and manual priorities. When the manual priority is set, the automatically deployed configuration will not overwrite the configuration manually modified by the user. 。
DHCP Option	
Option Value	Configure DHCP options to support automatic deployment application parameters using three methods: DHCP custom option, DHCP option 66, and DHCP option 43. When obtaining automatic deployment application parameters via DHCP, users can choose any one of these methods, with the terminal defaulting

	to DHCP option disable.
Custom Option Value	Custom Option value is allowed from 128 to 254. The option value must be same as server define.
Protocol Type	Transferring protocol type, supports FTP、TFTP、HTTP and HTTPS.
Enable DHCP Option 120	Use Option120 to get the SIP server address from DHCP server.
DHCPv6 Option	
Option Value	Configure DHCP options to support obtaining automatic deployment application parameters using three methods: DHCP custom option, DHCP option 66, and DHCP option 43. When obtaining automatic deployment application parameters via DHCP, users can choose any one of these methods, with the terminal defaulting to DHCP option 66.
Custom Option Value	Custom Option value is allowed from 128 to 254. The option value must be same as server define.
SIP Plug And Play（PnP）	
Enable SIP PnP	Whether enable PnP or not. If PnP is enabled, phone will send a SIP SUBSCRIBE message with broadcast method. Any server can support the feature will respond and send a SIP Notify with URL to phone. Phone could get the configuration file with the URL.
Server Address	Configure the PnP server.
Server Port	Configure PnP port.
Transport Protocol	Configure PnP protocol.
Static Provisioning Server	

Server Address	Configure the address of the FTP server. The server address can be in IP format, such as 192.168.1.1, or in domain name format, such as ftp.domain.com. Additionally, the system supports the functionality of setting subdirectories for the server. For example, the system can configure the server address in the form of 192.168.1.1/ftp/Config/ or ftp.domain.com/ftp/config. This means that the accessed server address is either 192.168.1.1 or ftp.domain.com, and the file storage path is under /ftp/Config/. The subdirectory can have or not have a "/" at the end.
Configuration File Name	Configure the name of the configuration file to be upgraded. Typically, when using the automatic upgrade feature, this field is left blank. In this case, the device will use its own MAC address as the filename to retrieve the file from the server.
Protocol Type	Transferring protocol type ， supports FTP、TFTP、HTTP and HTTPS.
Update Interval	Configure the time for interval upgrades, with the unit being hours.
Update Mode	Provision Mode: 1. Disabled. 2. Update after reboot. 3. Update after interval.
Auto provision Now	
TR069	
Enable TR069	Enable TR069 after selection.
ACS Server Type	Select ACS server type. The terminal currently supports two types of ACS servers: telecom and regular.
ACS Server URL	ACS server address.
ACS User	ACS server authentication username.
ACS Password	ACS server authentication password.
Enable TR069 Warning Tone	If TR069 is enabled, there will be a prompt tone when connecting.
TLS Version	TLS Version(TLS 1.0, TLS 1.1, TLS 1.2)

INFORM Sending Period	Configure the cycle interval, with the unit being seconds.
STUN Server Address	Enter the STUN address.
STUN Enable	Enable the STUN.

8 Preference Settings

8.1 Time Settings

Users can set the time and date through both the device's web interface.

Web Interface for Setting Time/Date:

Users can set the device's time and date by going to the web page **[Device Settings] >> [Time/Date].**

Parameters:

Parameter	Description
Network Time Server Settings	
Time Synchronized via SNTP	Enable time-sync through SNTP protocol.
Time Synchronized via DHCPv6	Enable time-sync through DHCPv6 protocol.
Time Synchronized via DHCP	Enable time-sync through DHCP protocol.
Primary Time Server	Set primary time server address.
Secondary Time Server	Set secondary time server address, when primary server is not reachable, the device will try to connect to secondary time server to get time synchronization.
Time zone	Select the time zone.
Resync Period	Time of re-synchronization with time server.
Time/Date Format	
12-Hour Clock	Set the time display in 12-hour mode.
Time/Date Format	Select the time/date display format.
Daylight Saving Time Settings	
Location	Choose your location, phone will set daylight saving time automatically based on the location.
DST Set Type	The daylight saving time rule based on specific dates or relative rule dates. In automatic mode, it is displayed as read-only.

Offset	The time adjustment applied when daylight saving time starts/ends.
Month Start	The DST start month.
Week Start	The DST start week.
Weekday Start	The DST start weekday.
Day Start	The DST start day.
Hour Start	The DST start hour.
Month End	The DST end month.
Week End	The DST end week.
Weekday End	The DST end weekday.
Day End	The DST end day.
Hour End	The DST end hour.
Manual Time Settings	You can set your time manually.

8.2 Audio Settings

8.2.1 Volume Settings

Users can adjust the device volume through both the web page .

Web interface for setting volume:

Users can set the device's volume through the web page **[Device Settings] >> [Media Settings] >> [Media Settings]**. After setting, click **[Apply]** to save.

Volume parameters：

- Speakerphone Ring Volume：Set the ringtone volume in hands-free mode.
- Speakerphone SignalTone Volume：Set the volume of incoming and outgoing signal tones. Set the volume of hands-free calls.
- Speakerphone Volume：Set the volume of hands-free calls.

8.2.2 Tone Setting

Users can set call alerts, call prompt tones, ringback tones, and reminder tones via the web page **[Device Settings] >> [Features] >> [Tone Settings]**.

Parameters	Description
Enable Holding Tone	When enabled, a prompt tone will be played during a call hold.
Enable Call Waiting Tone	If this function is turned off, you won't hear the "beep-beep" prompt sound when there is a call waiting.
Play Dialing DTMF Tone	When users press the device's numeric keys during dialing, there will be DTMF tone prompts.
Play Talking DTMF Tone	When the user presses the device's numeric keys during a call, DTMF prompt tones will be heard. This feature is enabled by default.
Boot Up Tone	A tone when the device is powered on
Ring Back Tone	The user can turn off the prompt tone or use a custom one.
Custom Ringback Sound	It supports custom ringback tones. In **[System] >> [Upgrade] >> [Ringtone Upgrade]**, after upgrading the ringtone file, you can use the setting under ringback tones to customize it.
Busy Tone	When the other party hangs up at the end of a call, the user can use the custom prompt tone for hanging up.

8.2.3 Ring Setting

Web interface setting:

Users can set the device ringtone type through the web page **[Device Settings] >> [Media Settings] >> [Media Settings]**. After setting, press **[Apply]** to save.

8.2.4 Upload Ring

Users can upgrade ringtone files through the web page **[System] >> [Upgrade] >> [Ring Upgrade]**. Once upgraded, the new ringtones will be displayed in the ringtone list.

Ring file format:

- Supports WAV,mp3,etc.tar.gz formats.
- The maximum size for a single file is 1M

9 Function Key Settings

9.1 Function Key Settings

Function Key Settings

Users can configure Function Key through the web page.

Web Interface Configuration of Function Key:

Access the device web page **[Function Key] >> [Function Key]**, configure the DSSKEY buttons, select button type as Memory Key/Key Event/DTMF, assign the configuration to the corresponding device, and then update.

Parameters	Description
Function Key Settings	
Memory Key	**Speed Dial**:Users can directly dial the set numbers. This function facilitates customers to dial frequently used numbers. **Intercom**: This feature allows operators or secretaries to connect calls quickly, and it is widely applied in office environments. **SOS**： Emergency call is often used for urgent alarms. Once the call is triggered, it can connect to the alarm center. However, the sound from the alarm center cannot be heard.
Key Event	Users can select a function key as a shortcut to trigger an event. For example: handfree, volume up, volume down, etc.
DTMF	When making a call, pressing this button can send the configured DTMF.
MCAST Paging	Configure the multicast address and voice encoding. Users can initiate a multicast by pressing this key.
Action URL	Users can use a specific URL to perform basic operations such as making calls and opening doors on the device.
MCAST Listening	When the device is on standby, if the function key is pressed and the RTP (Real-time Transport Protocol) of the multicast is detected to be present, the device will monitor that multicast.
PTT	**Speed Dial**： When pressed, it initiates a call for a conversation, and when

	released, it ends the call. **Intercom**：When pressed, it initiates an intercom call for communication, and when released, it ends the intercom call. **Multicast**： When pressed, it initiates a multicast for multicast anti-skid purposes, and when released, it terminates the multicast.
Programmable Key Settings	
Desktop	None: There is no response when the button is pressed. Dsskey1：When it is set as DSSKey1, operations such as making calls and answering calls are carried out according to the settings of DSSKey1. Dsskey2：When it is set as DSSKey2, operations such as making calls and answering calls are carried out according to the settings of DSSKey2. Dsskey3：When it is set as DSSKey3, operations such as making calls and answering calls are carried out according to the settings of DSSKey3.
Dialer	None: There is no response when the button is pressed. Dsskey1：When it is set as DSSKey1, operations such as making calls and answering calls are carried out according to the settings of DSSKey1. Dsskey2：When it is set as DSSKey2, operations such as making calls and answering calls are carried out according to the settings of DSSKey2. Dsskey3：When it is set as DSSKey3, operations such as making calls and answering calls are carried out according to the settings of DSSKey3.
Ringing	Invalid: When the button is pressed during ringing, there will be no response at all. Answer: When set to "Answer", in the event of an incoming call, if the automatic answering function is not enabled, pressing the button allows you to answer the incoming call. End: When set to "End", when there is an incoming call, pressing the button can hang up the incoming call.
Alerting	Invalid: When making an outgoing call, pressing the button will not trigger any response. End: When it is set to "End", when making an outgoing call, pressing the button can hang up the call.
Talking	End: When set to "End", when there is a call in progress, pressing the button

	will end the call. Volume Up: When set as the volume up key, during a call, pressing the key can increase the volume. Volume Down: When set as the volume down key, during a call, pressing the key can decrease the volume. Dsskey1：When it is set as DSSKey1, operations such as making calls and answering calls are carried out according to the settings of DSSKey1. Dsskey2：When it is set as DSSKey2, operations such as making calls and answering calls are carried out according to the settings of DSSKey2. Dsskey3：When it is set as DSSKey3, operations such as making calls and answering calls are carried out according to the settings of DSSKey3.
Desktop Long Pressed	Invalid: Long pressing the button has no response. Main Menu: Long press the call button to enter the command mode.
Advanced Settings	
Dial Mode Select	Mode selection for forwarding calls from number 1 to number 2. <Main-Secondary>: If the first number does not answer within the set time, the call will be automatically switched to the second number. <Time Period>: Automatically detect the system time during a call. If it is within the time slot of number 1, call number 1; otherwise, call number 2. <Group Call>: Dial out all the set numbers at the same time. Once one of the numbers is answered, the calls to the other numbers will be hung up.
Call Switched Time	Set the time for forwarding from number 1 to number 2. The default time is 16 seconds.
First Number Start Time	When defining the time period mode, the start time of number 1. The default is "06:00".
First Number End Time	When defining the time period mode, the end time of number 1. The default is "18:00".
Use Function Key Name in Display Name	Use the name of the set shortcut key as the display name and send it to the peer device.

10 Network Settings

10.1 Ethernet Connection

Users can set up wired networks through the device's web page and device menu. The device defaults to using IPv4 mode, and users can refer to the Network Mode to modify the network mode.

Setting up wired networks through the web interface:

Users can access the web page and go to **[Network] >> [Basic] >> [IPv4 Settings]** to configure the network type. Both static IP and DHCP configurations are supported.

Setting up wired networking through the device menu (H6W only):

Users can configure the network type via the device menu by going to **[System] >> [Network].** Both static IP and DHCP configurations are supported.

To set a static IP:

When the network is set to use a static IP, the device allows you to manually configure the IP address.

- IP address: Enter the IP address you wish to set.
- Subnet mask: Set the subnet mask.
- Default gateway: Used for network interconnection, fill in according to your needs.
- Primary DNS Server: The IP address of the primary DNS server.The default is 8.8.8.8, provided for free by Google.
- Secondary DNS Server: The IP address of the secondary DNS server.

10.2 Wireless Network（Only H501W）

The device supports wireless internet access. There are two ways to connect to Wi-Fi: Set up a wireless network connection in **[Network] >> [Wi-Fi Settings]** on the device's web page.

Connect through the web interface ：

Log in to the device's web page, enable Wi-Fi in the **[Network] >> [Wi-Fi Settings]** interface. After adding the Wi-Fi information, click [Add]. Then you can see the connected Wi-Fi in the wireless network list.

Connect through another device:

Method 1:

- Enter **[Advanced Settings]** on the W611W, then go to **[Share Wi-Fi]** to enable the Wi-Fi sharing function and set the office network SSID and password. At this point, the W611W functions as an AP.
- Power on the H501W devices.
- After powering up, the W611W will push the office network SSID and password to the H501W, enabling them to connect to the office network.

Method 2:

- The user creates a Wi-Fi network with the SSID "**WiFi-device-ssid**" and the password "**i<0%aY8+**".
- After powering on, the H501W devices will automatically connect to this Wi-Fi.
- The Wi-Fi information of the H501W can be modified through automatic deployment to connect to the office network.
- Wi-Fi module configuration file as shown:

```
<<VOIP CONFIG FILE>>Version:2.0000000000

<NET CONFIG MODULE>

--WIFI List--     :
Item1 WIFI Name         :Redmi K60
Item1 WIFI SSID         :Redmi K60
Item1 Secure Mode       :1
Item1 WIFI Encryption   :1
Item1 WIFI User Name    :
Item1 WIFI Password     :12345678

<<END OF FILE>>
```

10.3 Network Mode

There are three IP Mode options available: IPv4, IPv6, and IPv4 & IPv6.Users can set up

wired network modes through the device's web page and device menu. Each network mode supports configuring the network type, either using static IP or DHCP.

Configure wired network modes through the web interface:

Users can access the web page and navigate to **[Network] >> [Basic] >> [Network Mode]** to set the network mode. Supported options include IPv4, IPv6, and IPv4 & IPv6.

10.4 Network Server

Users can configure network service types via the web page by navigating to **[Network] >> [Service Port]**.

Parameter	Description
Web Server Type	Changes take effect after a restart. You can choose the web login to be either HTTP or HTTPS.
Web Logon Timeout	Default is 15 minutes. After this time, the login session will automatically expire, requiring a new login.
Web Auto Login	After timeout, re-login to the web page does not require entering username and password; it will automatically log in.
HTTP Port	Default is 80. For enhanced system security, you can set a port other than 80, such as 8080. Web login would be: HTTP://IP:8080
HTTPS Port	Default is 443, used in the same way as the HTTP port.
RTP Port Range Start	The value range is from 1025 to 65535. The RTP port starts from the initial value set, and for each call, the values of the voice and video ports increase by 2.
RTP Port Quantity	The number of calls

10.5 VPN

Feature Description:

- Virtual Private Network (VPN) is a technology that allows devices to create a connection to a server and become part of the server's network. The network transmission of the indoor unit can be connected through the VPN server routing function.
- For some users, particularly corporate users, it may be necessary to establish a VPN connection before activating line registration. The device supports two VPN modes: Layer 2 Tunneling Protocol (L2TP) and OpenVPN.
- Users must enable (or disable) and configure the VPN by logging into the web page.

L2TP Setup Method:

- Visit the web page **>> [Network] >> [VPN]**, enable VPN mode, select "L2TP" as the type, and then fill in the L2TP server address, L2TP authentication username, and authentication password. Click "Apply" and the phone will attempt to connect to the L2TP server.
- When establishing a VPN connection, the VPN IP address will be displayed in the VPN status area. There may be delays in establishing the connection. Users need to refresh the page to update the status timely.
- Once the VPN configuration is successful, the indoor unit will automatically attempt to connect to the VPN each time unless disabled. Sometimes, if the VPN connection is not established promptly, users can try restarting the device and check if the VPN has been successfully established after the restart.

Note:

The device only supports basic unencrypted authentication and data transmission. If users require data encryption, please use the OpenVPN feature instead.

To set up an OpenVPN connection, follow these steps:

- Obtain authentication and configuration files from your OpenVPN service provider. The files required include:

- OpenVPN Configuration file: client.ovpn
- CA Root Certification:ca.crt
- Client Certification:client.crt
- Client Key:client.key

- Upload the files listed above to the Manager's webpage under **[Network] >> [VPN]**, and select the OpenVPN files.
- Go to the device webpage, navigate to **[Network] >> [VPN]**, enable VPN mode, choose **"OpenVPN"** as the type, and submit the information to activate the OpenVPN feature.

Like the L2TP connection, the system will attempt to establish a connection upon every system restart until manually disabled by the user.

10.6 VLAN

VLAN (Virtual Local Area Network) technology allows a LAN to be divided into multiple logical LANs—VLANs, each VLAN being a broadcast domain where broadcast messages are confined within a single VLAN.

Support is provided for acquiring VLAN ID via LLDP, CDP, DHCP, and manual settings.

LLDP (Link Layer Discovery Protocol)

- Access the device web page **>> [Network] >> [Advanced] >> [Link Layer Discovery Protocol]**, configure LLDP settings:
  - Enable LLDP: Activate the LLDP protocol function
  - Packet Interval: Set the send interval for LLDP discovery packets
  - Enable Learning Function: Enable LLDP to autonomously learn VLAN configuration settings

CDP (Cisco Discovery Protocol)

- Access the device web page **>> [Network] >> [Advanced] >> [Cisco Discovery Protocol]**, configure CDP settings:
  - Enable CDP: Activate the CDP protocol function
  - Packet Interval: Set the send interval for CDP discovery packets

DHCP VLAN

- Access the device web page **>> [Network] >> [Advanced] >> [DHCP VLAN Settings]**, configure DHCP VLAN parameters:
  - Selection of Option Value: Enable or disable acquiring the VLAN ID through DHCP OPTION.
  - DHCP Option VLAN: Set the OPTION value, 128-254, to obtain the VLAN value via DHCP.

Manual VLAN Setup

- WAN VLAN Settings: Access the device web page **>> [Network] >> [Advanced] >> [WAN VLAN Settings]**, manually configure the WAN VLAN ID:
  - Enable VLAN: Activate the manual setting of the WAN VLAN function.
  - WAN VLAN ID: Set the WAN VLAN ID.

802.1x Settings

- Access the device web page **>> [Network] >> [Advanced] >> [802.1x Settings]**,configure 802.1x parameters:
  - 802.1x Mode: Select the 802.1x authentication mode or disable authentication.
  - Identify: Set the authentication username.
  - Password: Set the authentication password
  - CA Certifiate: Upload the CA Certificate
  - Device Certificate: Upload the Device Certificate

Certification File

- Access the device web page **>> [Network] >> [Advanced] >> [Certification File],** Users can customize and upload HTTPS certificate files.

11 Security

11.1 Web Password

Via the user interface to modify the password:

Users can customize and change the web login password by clicking on the option in the upper-right corner Default password is in use. Please change! and then selecting **[Change Web Authentication Password]** after logging into the web page.

Modify the web page password parameter settings:

- Old Password: Enter the web page login password.
- New Password: Enter the new login password you wish to set.
- Confirm Password: Please enter the new login password again for confirmation.

After the password is modified, the system will automatically log out, and you will need to enter the new password to log in again.

11.2 Web Filter

Users can configure to allow only machines from a specific IP subnet to access and manage the configuration of the device.

Navigate to the web page **[Security] >> [Web Filter],** add or delete allowed IP subnets. Configure the starting and ending IP addresses within the specified range, then click **[Add]** to apply the changes. You can set a large subnet or add multiple subnets. When deleting, choose the starting IP of the subnet you want to remove from the dropdown menu, and then click **[Delete]** to apply the changes.

Enable Web Filtering: Configure to enable/disable web access filtering. Click the **[Apply]** button to apply the changes.

Note：

If accessing the device from a machine within the same subnet, do not configure the web filtering subnet to be outside of your own subnet; otherwise, you won't be able to log in to the webpage.

11.3 Mutual Authentication

The device supports mutual authentication using HTTPS and SIP TLS.

Certificate Management

- Device Certificate: Access the web page **[Security] >> [Device Certificates]** to set the device certificate parameters:
  - Device Certificates: Choose the device certificate to be used for authentication, which can be either the default certificate built into the device or a custom certificate uploaded by the user.
  - Import Certificates: Upload a custom device certificate.
  - Certificate File: Displays the list of uploaded custom device certificates. Only one custom device certificate can be uploaded. If no custom certificate is uploaded, the certificate list will be empty.
- Trusted Certificates: Access the web page **[Security] >> [Trusted Certificates]** to set the trusted certificates parameters:
  - Permission Certificate: Used to decide whether to enable server certificate verification.
  - Common Name Validation: Option to enable or disable common name validation.
  - Certificate Module: Select the certificate module to be used, with the following options:
    - All Certificates: Trusts all certificate modules, including both the custom uploaded trusted certificate list and the built-in trusted list in the device.
    - Default Certificates: Trusts the built-in trusted certificate list of the device.

- ✧ Custom Certificates: Trusts the custom uploaded trusted certificate list.

➢ Import Certificates: Used to import trusted certificates from the server side.

➢ Certificate List: Displays the list of custom uploaded server trusted certificates.When no custom certificate is uploaded, the certificate list will display as empty.

Mutual Authentication Explanation

- Upload the device certificate used to the server's trusted certificate list, ensuring that the server's trusted certificate list includes the device's certificate. Please confirm with the server administrator.
- Access the web page **[Security] >> [Trusted Certificates] >> [Import Certificates]** to upload the server's device certificate to the device's trusted certificate list and select the trusted certificate module to use.

11.4 Network Firewall

Setting the Network Firewall

- Access the device's web page >> **[Security] >> [Firewall]**, where you can set whether to enable the inbound and outbound firewall. You can also define rules for the inbound and outbound traffic through the firewall. These settings help prevent malicious network access and restrict internal users from accessing certain external network resources, thereby enhancing security.

Feature Description

- The firewall rule setting is a simple firewall module that supports two types of rules: inbound rules and outbound rules. Each rule is assigned a sequence number, with a maximum of 10 rules allowed for each type.
- Once the parameters are set, clicking **[Add]** will add a new item to the firewall's outbound rules.
- To delete an item, select the desired list and click **[Delete]** to remove the selected list.

Parameters:

Parameter	Description
Enable Input Rules	Indicates that the input rule application is enabled.
Enable Output Rules	Indicates that the output rule application is enabled.
Input/Output	To select whether the currently added rule is an input or output rule.
Deny/Permit	To select whether the current rule configuration is disabled or allowed.
Protocol	There are four types of filtering protocols: TCP | UDP | ICMP.
Filter port range	The range of filtered ports
Src Address	Source address can be host address, network address, or all addresses 0.0.0.0; It can also be a network address similar to *.*.*.0, such as: 192.168.1.0.
Dst Address	The destination address can be either the specific IP address or the full address 0.0.0.0; It can also be a network address similar to *.*.*.0, such as: 192.168.1.0.
Src Mask	Is the source address mask. When configured as 255.255.255.255, it means that the host is specific. When set as 255.255.255.0, it means that a network segment is filtered.
Dst Mask	Is the destination address mask. When configured as 255.255.255.255, it means the specific host. When set as 255.255.255.0, it means that a network segment is filtered.

12 Trouble Shooting

When the device is not in normal use, the user can try the following methods to restore normal operation of the device or collect relevant information and send a problem report to Fanvil technical support mailbox.

12.1 Get Device System Information

Users can obtain information through the device web page **[System]>>[Information]** options.The following information will be provided:

1. Device information (model, software and hardware version).
2. Account information.
3. Internet Information.

12.2 Reboot Device

Users can restart the device via the web interface or device menu.

Web Interface Restart:

Click on **[System] >> [Reboot]** and press **[OK].**

Power Cycle Restart:

Simply unplug the device and plug it back in to restart.

12.3 Device Factory Reset

Users can restore the device to default settings through the web interface or the device menu.

Web Interface Restore:

Click on **[System] >> [Configurations] >> [Reset Device] >> [Reset]** button and press **[OK]**.

12.4 Network Packets Capture

In order to obtain the data packet of the device, the user needs to log in to the web page

of the device, open the web page **[System] >> [Tools] >> [LAN Packet Capture]**, and click the **[Start]** option in the "Network Packets Capture".If you are using a Wi-Fi network, click the **[Start]** option in **[WLAN Packet Capture]**. A message will pop up asking the user to save the captured file. At this time, the user can perform related operations, such as starting/deactivating the line or making a call, and clicking the [Stop] button on the web page after completion. Network packets during the device are saved in a file. Users can analyze the packet or send it to the Technical Support mailbox.

12.5 Get Device Log

When encountering abnormal issues, log information can be helpful. The device supports exporting system logs and Wi-Fi logs.

Obtain system log:

To obtain the device's log information, users can log into the device's web page, navigate to **[System] >> [Tools] >> [Syslog]:**

- Set the system log to diagnostic mode.
- Enable log export and submit the changes.

Follow the steps where the issue occurs until it appears, then go to **[System] >> [Tools] >> [Export Log]** and click on export logs to save the logs locally for analysis or send them to technical staff for problem resolution.

Obtain Wi-Fi Log:

To obtain the device's Wi-Fi log information, users can log into the device's webpage, navigate to **[System] >> [Tools] >> [WLAN Logs]**

- Enable WLAN logging and submit the changes.

Follow the steps where the issue occurs until it manifests, then go to **[System] >> [Tools] >> [WLAN Logs]** and click on export logs to save the logs locally for analysis or send them to technical staff for problem resolution.

12.6 Common Trouble Cases

Trouble Case	Solution
Device could not boot up	1. The device is powered by a power adapter. Please use a compliant power adapter and check if the device is connected to power. 2. The device is powered by PoE. Please use a compliant PoE switch.
Device could not register to a service provider	1. Please check if the device is connected to the network. 2. Verify if the device has an IP address. Check the system information; if the IP address is 0.0.0.0, it indicates that the device has not obtained an IP address. Ensure that the network configuration is correct. 3. If the network connection is fine, recheck your cable configuration. If all configurations are correct, contact your service provider for support, or follow the instructions in 12.4 Network Packets Capture to obtain network packets for analysis. Send them to the support email to help diagnose the issue.

13 Appendix Table

13.1 Appendix I - Indicator Light

Type	LED	Status
Status Light	Quick Flashing	Registration failed、Abnormal network
	Slow Flashing	Talking/Calling/Ring
	Normally on	Successfully registered

13.2 Appendix II - Command Mode

Action	Description
Report IP when in standby mode	When the device is in standby mode, long-press the call button for 3 seconds. A prompt tone will sound. Within 5 seconds, press the call button again to report the IP address.
Switch Network Mode	When the device is in standby mode, long-press the call button for 3 seconds to enter the command mode. A prompt tone will sound. Within 5 seconds, quickly press the call button three times to switch the network mode； If there is currently no IP address, it will be switched to the default static IP address. When it is the default static IP address (192.168.1.128), it will be switched to the DHCP mode. When an IP address is obtained through DHCP, there will be no switching, and the IP address will be reported directly； After the network mode is successfully switched, the IP address will be reported.