i501(W)
User Manual

Version: 0.1 | Date: 2025.01.17

Connect

Safety Instruction

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.

Product Overview

Overview

The Fanvil i501/i501W is a high-cost-performance screenless indoor station that supports 2 SIP lines and features 1 short-circuit input interface. It is mainly used in residential communities, office buildings, and hotels to receive calls from door stations, conduct intercom communication, and remotely unlock the door station. It provides users with reliable security and convenient visitor call services, creating a safe and comfortable living environment.

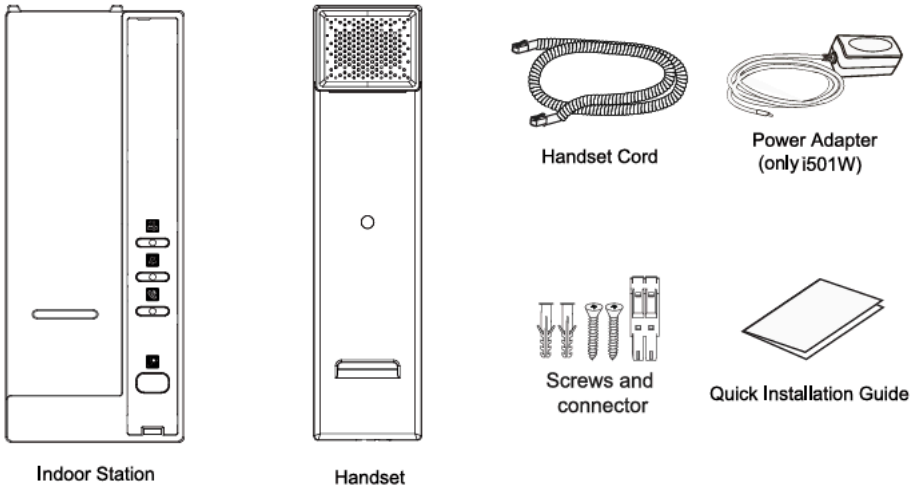
In order to help some interested users to better understand the details of the product, the user manual can be used as a reference guide for the use of i501/i501W. This document may not apply to the latest version of the software. If you have any questions, you can use the help prompt interface that comes with the i501/i501W device, or download and update your user manual from the official website.

Specification Parameter

Spec.	i501	i501W
Material	ABS	
Wi-Fi	/	2.4G
Speaker	1W	
Interface	1 × short-circuit input	
Network	10/100 Mbps adaptive	
Operating temperature	0℃~50℃	
Size (LWH)	mm	
Wall-mounted	Support	

Installation Instruction

Device Inventory



Note: The i501W comes with a standard power adapter, while the i501 supports PoE for both network connectivity and power supply.

Installation Procedure

Wall-mounted

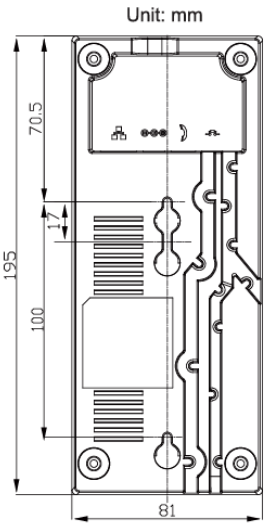
Please install the indoor station according to the instructions provided in the image below:

Drill two holes in the wall, the vertical distance between the two holes is 100mm;

Drive in screw anchors and screws in turn; Note: 5mm is reserved between the screw cap and the wall for easy installation of the phone base;

Connect the Ethernet cord, handset cord and power;

Align the wall mounting holes on the base with the screws made in step 2, slide down to complete the installation.



Wi-Fi Configuration St

Method 1:

Enable **[Share Wi-Fi]** on W611W: Gc **ced Settings] >> [Share Wi-Fi]**. Turn on the Wi-Fi sharing feature and configu sword for the office network. At this point, the W611W functions as an AP.

Power on the i501W device.

After powering on, the W611W will push the office network's SSID and password to the i501W, enabling it to connect to the office network. When the Wi-Fi connection is successful, the power indicator will

flash red five times quickly.

Method 2:

The user creates a Wi-Fi network with the SSID WiFi-device-ssid and password i<0%aY8+.

After powering on, the i501W device automatically connects to this Wi-Fi.

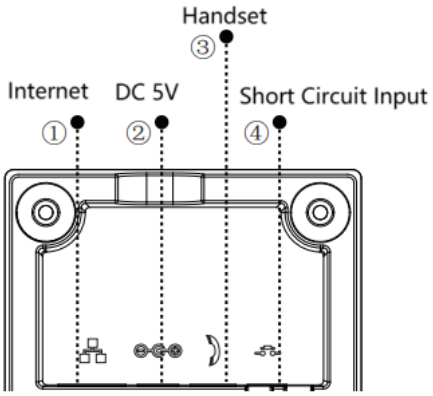
Upon successful connection, the power indicator will flash red quickly five times. The Wi-Fi information of the i501W can then be updated to connect to the office network using automatic deployment.

The Wi-Fi module configuration file is as follows:

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

<NET CONFIG MODULE>

--WIFI List--      :
Item1 WIFI Name         :WiFi-test
Item1 WIFI SSID         :WiFi-test
Item1 Secure Mode       :1
Item1 WIFI Encryption   :1
Item1 WIFI User Name    :
Item1 WIFI Password     :12345678

<<END OF FILE>>
```

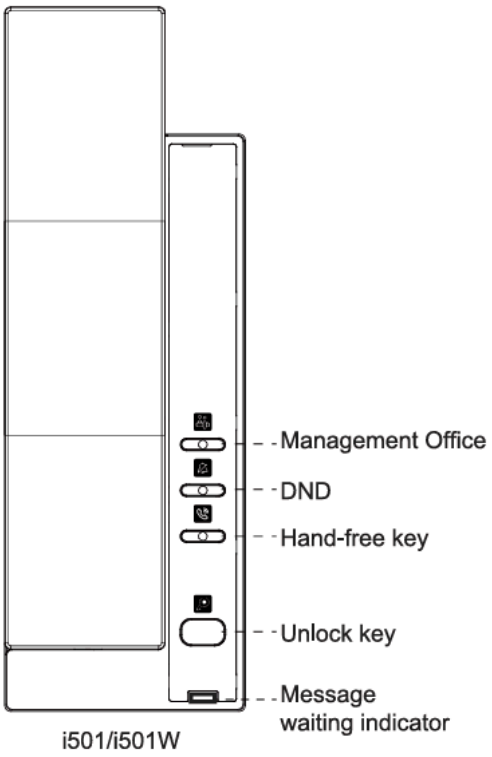
User Guide

Interface Instruction



Number	Name	Description
①	Network Port	Connect to a local area network (LAN) or the Internet.
②	Power Port	Connect the power adapter.
③	Handset Port	Connect the device handset.
④	Short-Circuit Input Port	Configurable short-circuit input function for door unlocking and more.

Button Instruction



i501/i501W

Number	Name	Description
①	Management Office	Customizable button, default set for speed dial, immediately dials the management office when pressed.
②	DND	Customizable button, default set to Do Not Disturb, can reject incoming calls.
③	Hands-free key	The user can press this button to enable or disable the hands-free speaker audio channel.
④	Unlock key	The custom button is set to the default as the door unlock button, which allows for one-click door unlocking when pressed.
⑤	Message waiting indicator	Power Indicator/Line Status Indicator.

Device Status

Users can view the device status via the web interface.

Log in to the web interface and navigate to **[System] >> [Information]** to check the device status:

System Information: Displays the device model name, hardware version, software version, uptime, memory information, system time, and other details.

Network: Displays the device's network mode, MAC address, Wi-Fi IP, subnet mask, gateway, and

related details.
Account: Displays the registered account name/number and registration status.

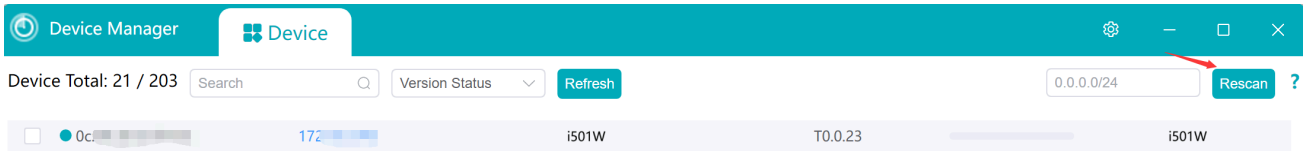
Web Management

Device IP Address

Retrieve Device IP through Scanning Tool:

Connect the computer and the i501W to the same local area network (LAN), and install Device Manager on the PC.

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



Obtain the device IP address directly from the device:

In standby mode, press and hold the first button  , and the device will announce the IP address via voice prompt.

Web Interface

Ensure the computer and device are on the same local network. Open a browser and manually enter the device's IP address, or click the IP address directly in the scanning tool interface to redirect to the browser. Enter the correct username and password on the login page. The default username and password are both "admin."

Language Settings

Users can set the language through the web interface.

Log in to the device's web page and select the desired language from the dropdown menu in the upper right corner 

. Check the "Sync language to the phone" option to ensure the language setting is applied to the device. After switching the web page language, the language used for IP announcements will also change accordingly.

Line Settings

The device supports two SIP accounts, allowing registration and seamless switching between them. Users can register SIP accounts through the web interface.

Navigate to **[Line] >> [SIP] >> [Line]** on the webpage to select the desired line for registration. Under **[Register Settings]**, configure the SIP parameters. Once the settings are complete, click **[Apply]** to successfully register the SIP account.

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.
Enable	The status of this line is 'Enabled'
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.

Call Features

Making Calls

Speed Dialing

When the user presses the shortcut key, it initiates a one-touch call.
To configure the shortcut key via the web interface:
Navigate to **[Function Key] >> [DSS Key]**, select **[Memory Key]** as the type, enter the SIP account or IP address, and choose **[Speed Dial]** as the subtype. In standby mode, pressing the configured key will immediately dial the assigned number.

Answer Call

Manual Answer

Users can answer calls by pressing the hands-free key or picking up the handset.

Auto Answer

Users can enable the auto-answer feature through the web interface. Once enabled, the phone will automatically answer incoming calls. Auto-answer can be enabled for specific lines. When disabled, the phone will ring for incoming calls and will not automatically answer after a timeout.

Enable auto-answer for the line:
Log in to the device webpage, navigate to **[Line] >> [SIP] >> [Basic Settings]**, check **[Enable Auto Answering]**, set the auto-answer time, and click apply.

Reject The Call

When the user ends the call, they can either return the handset or press the hands-free key to end the call.
For handset calls, hang up the handset to end the call.
For hands-free calls, press the hands-free key to end the call.

DND

The user can enable the Do Not Disturb (DND) feature on the device to reject incoming calls. After configuring it on the device's web interface, the user can activate it directly on the terminal device.

Set through the device web interface:

Access the device web interface >> **[Function Key] >> [Function Key]**, select **[Key Event]** as the type, and "Do-not-disturb" as the subtype. After configuring, click **[Apply]**.

Advance Function

Intercom

After activating the intercom mode, the device can automatically answer incoming calls in intercom mode.

Initiate Intercom

To use the intercom function, the function key needs to be set as a memory key - intercom button in advance. This can be configured through the device web interface.

To configure the intercom function key through the web interface:
Go to **[Function Key] >> [Function Key]**, select the key to configure, set the key type to **[Memory Key]**, the subtype to **[Intercom]**, and set the value, name, line, etc., then save the settings.

Intercom Call

Once the intercom mode is activated, the device will automatically answer incoming intercom calls.

Users can configure intercom-related parameters through the device's web interface by navigating to **[Phone Settings] >> [Function Settings] >> [Intercom Settings]**.

Configuration parameters:

Parameter	Description
Enable Intercom	When the intercom system is enabled, the device will automatically answer calls upon receiving the SIP header Call-Info command in the incoming call request.
Enable Intercom Mute	Enable the mute function during an intercom mode call.
Enable Intercom Tone	If the incoming call is intercom call, the phone plays the intercom tone.
Enable Intercom Barge	Enable Intercom Barge by selecting it, the phone auto answers the intercom call during a call. If the current call is intercom call, the phone will reject the second intercom call.

MCAST

The multicast feature allows for simple and convenient announcements to all multicast members by configuring the device to monitor a multicast address and play the RTP stream sent to that address.
Users can configure the multicast listening address and port through the web interface: **[Phone Settings] >> [MCAST]**.

Configuration parameters:

Parameters	Description
Priority	Defines the priority in the current call, with 1 being the highest priority and 10 the lowest.

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.
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:

Multicast configuration information can be delivered via SIP Notify signaling. Upon receiving the information, the device will configure it into the system to enable multicast listening or cancel multicast listening in the system.

Multicast Call:

Go to Web Interface **>> [Function Key] >> [Function Key]**, select Multicast as the key type, set the multicast address, and choose the codec.

After configuration, click **[Apply]**.

On the receiving phone's Web Interface **>> [Phone Settings] >> [MCAST]**, configure the multicast name, host, and port.

Press the configured DSS Key for multicast.

The receiving phone will accept the multicast call and automatically play the multicast audio.

Hotspot

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.

Server-side Settings:

Go to the device's web page: **[Line] >> [SIP Hotspot] >> [SIP Hotspot Settings]**. Enable hotspot settings as "Enabled", set the mode to "Hotspot", and assign a unique name that does not match any other hotspot server name.

After completing the settings, click **[Apply]**.

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.

Calling internal extension:

The hotspot server and client can dial each other through the extension number before.

Extension 1 dials extension 0.

Message

MWI

If the server on this line supports voicemail functionality, the caller can leave a voicemail on the server when the user does not answer. To listen to voicemails, the user must first configure the voicemail number. After configuring the voicemail number, the user can retrieve voicemails from the default line.

Users can configure the power indicator's display status for received voicemails via the web interface: **[Phone Settings] >> [Features] >> [Power LED]**.

Listen to voicemail:

To listen to voicemail, you must enable voicemail for that line and fill in the voicemail retrieval number. Users can enable and fill in this information on the web page **[Line] >> [SIP] >> [Basic Settings] >> [Voice Message Number]**.

Users can configure the voicemail function key on the web page **[Function Key] >> [Function Key]**. Select **[Key Event]** as the type and **[Voice Mail]** as the subtype. After configuration, users can press the voicemail function key to call the voicemail number, follow the prompts to enter the PIN code, and listen to their voicemail.

Open Door

The indoor station can operate the door access control system to open the door while in standby mode or during a call.

Open The Door Under Standby

In standby mode, the user can press the **[Open Door]** button  on the device to open the door.

Settings Of Open The Door Under Standby

The user can configure the settings through the web interface:
Navigate to **[Function Key] >> [Function Key]**, set the type to URL, enter the name and value, and click **[Apply]** to save.

Open the door during a call

During a call, the user can press the **[Open Door]** button  on the indoor station to open the door. Once pressed, the door connected to the intercom system will unlock while the call is active.

Open The Door During A Call

Steps to unlock the door during a call:
Establish a call with the door access system.

During the call, press the **[Open Door]** button  to unlock the door.

Settings Of Open The Door During A Call

Users can configure the Open Door button via the web interface:
Navigate to **[Function Key] >> [Function Key]**, set the type to DTMF, enter the name and value, and click **[Apply]** to save.

Call Log

Web interface for viewing call logs:

Viewing : The system can store up to 1000 call records. Users can view the call logs by navigating to **[Call Logs] >> [Call Information]**, where they can access records of all incoming, outgoing, forwarded, and missed calls.

Deleting: Users can delete call records by selecting the desired records or selecting all, then clicking the **[Delete]** button to remove them.

Exporting: Users can select the call records they wish to export, or select all, and then click the **[Export]** button to export the records.

Device Settings

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 **[Phone 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.

Parameters:

Parameters	Description
Name	Enter a defined action name.
Type	Timed reboot, Timed upgrade, Timed forward, Timed Config
Repetition period	No repetition: Execute once within the configured time range. Daily: Perform this operation at the same time range every day. Weekly: Perform this operation within the specified time range on selected days of the week. Monthly: Perform this operation within the specified time range on specific dates of the month.
Start date	The date when it takes effect.
End date	The date when it ends.
Effective Time	Set the time period for execution.

Note:
If the set time period is fully occupied with calls, the reboot or upgrade operation will be skipped.

Action Plan

Action Plan application: A technology defined and designed by Fanvil for remote control and behavior linkage between Fanvil terminal devices and other devices. When an event occurs on a Fanvil terminal, the terminal can execute an action based on a predefined 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	When the number configuration rule is triggered, the following actions can be performed: **MCAST-Xfer**: When the trigger rule is activated, the phone converts incoming calls or multicast to multicast and sends them to the configured multicast address and port. **Mute**: The phone will automatically mute when the rule is triggered. **Answer**: The phone will automatically answer the incoming call when the rule is triggered.
Number	Each Action Plan corresponds to a call number and supports the same number expression as the Dial Plan.
Type	**Connected**: Triggered and executed after the call is established.
Line	The selected rule corresponds to the matching SIP line.
Direction	The behavior handling method corresponding to the configured rule: **Both**: Triggered for both incoming and outgoing calls. **Outgoing Call**: Triggered on outgoing calls. **Incoming Cal**l: Triggered on internal incoming calls.
Username	RTSP Authentication Username
Password	RTSP Authentication Password

Maintenance

Configurations

On this page, 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" (note: profile export requires administrator privileges).

Import Configurations

Import the configuration file of Settings.

Clear Configuration

Clear configurations related to SIP, auto-deployment, shortcuts, etc.

Clear User Data

Clear configurations related to SIP, auto-deployment, shortcuts, etc.

Clear ETC

Clear certificate. Valid Value:Contains HTTPS and VPN certificates.

Reset Phone

Reset phone to factory default settings.

Upgrade

Web Upgrade

Upgrade Device Software Version: Upgrade to the new version via the web. Once the upgrade is complete, the device will automatically restart and update to the new version.

Go to **[System] >> [Upgrade],** select a file, choose the version, and click **"Upload"** to proceed.

Online Upgrade

Through online upgrading, devices can be upgraded.
Configuration for online upgrades by an administrator through a 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.

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 Version information	
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 information	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.

Instructions:

After completing the configuration on the Manager web page, place the version information TXT file into the configured HTTP server. The naming format for the version information TXT file should be: vendor_model_hwv1_0.txt

After completing the configuration on the Manager web page, place the version information TXT file into the configured HTTP server. The naming format for the version information TXT file should be: vendor_model_hwv1_0.txt:

```
Version=2.12.0  #Software Version Number
Firmware=http://ip:port/xxx.z    #URL of the Software Version File
BuildTime=2023.09.11 20:00
```

Info=TXT

Release Note:
Xxxxx
Xxxxx
Xxxxx

After the update interval has elapsed, if the server has available TXT files and version files, the device UI will indicate that a new version file is available. Users can click to upgrade to the new version; the web page will show an enabled upgrade button along with the Release Note from the TXT file, allowing users to click and upgrade the version.

Auto Provision

Webpage: 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。

Parameters	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	The password of provision server.
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	When the feature is enable, if the configuration of server is changed, phone will download and update.

Provision Config Priority	The Settings of the upgrade pop-up are displayed.
DHCP Option	
Option Value	Configure DHCP option, DHCP option supports DHCP custom option | DHCP option 66 | DHCP option 43, 3 methods to get the provision URL. The default is Option 66
Custom Option Value	Custom Option value is allowed from 128 to 254. The option value must be same as server define.
Enable DHCP Option 120	Use Option120 to get the SIP server address from DHCP server.
DHCPv6 Option	
Option Value	Configure DHCPv6 option, DHCPv6 option supports custom option | option 66 | option 43, 3 methods to get the provision URL. The default is Disable.
Custom Option Value	Custom option number. Must be from 128 to 254.
SIP Plug and Play	
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 Notify with URL to phone. Phone could get the configuration file with the URL.
Server Address	Broadcast address.
Server Port	PnP port。
Transport Protocol	PnP protocol, TCP or UDP.
Update Interval	Configuration file update interval time. As default it is 1, means phone will check the update every 1 hour.
Static Provisioning Server	
Server Address	Configure the address of the FTP server to be set up. The server address can be in the form of an IP address, such as 192.168.1.1, or a domain name, such as ftp.domain.com. The system also supports the configuration of subdirectories for the server. For example, the server address can be set in the format 192.168.1.1/ftp/Config/ or ftp.domain.com/ftp/config, meaning that the server address is 192.168.1.1 or ftp.domain.com, and the file storage path is /ftp/Config/. The presence or absence of a '/' at the end of the subdirectory is acceptable.
Configuration File Name	Configure the name of the configuration file to be upgraded. Generally, when using the auto-upgrade function, this field is left blank. In this case, the device will use its own MAC

	address as the file name to retrieve the file from the server.
Protocol Type	Transferring protocol type，supports FTP、TFTP、HTTP and HTTPS.
Update Interval	Configure the interval for upgrades, in hours.
Update Mode	Provision Mode: 1.Disabled. 2.Update After Reboot 3.Update at Time Interval
Autoprovision Now	
TR069	
Enable TR069	Enable TR069 after selection
ACS Server Type	Select the type of ACS server.
ACS Server URL	ACS server address
ACS User	ACS server username
ACS Password	ACS server password
Enable TR069 Warning Tone	If TR069 is enabled, there will be a prompt tone when connecting.
TLS Version	If auto-login is selected, the device will not prompt for a username and password upon reboot. Instead, it will use the previously entered correct username and password to connect to the ACS server.
STUN Server Address	Enter STUN address
STUN Enable	Enable STUN

Preferences

Audio Settings

Ring Setting

Web interface for setting ringtones:
The user can set the device ringtone type through the webpage **[Phone Settings] >> [Media Settings] >> [Media Settings]**. After making the settings, click **[Apply]** to save.

Volume Setting

The user can set the device volume through the webpage.

Web interface volume setting:
The user can set the device volume through the webpage **[Phone Settings] >> [Media Settings] >> [Media Settings]**. After making the settings, click **[Apply]** to save.

Volume parameters:
Handset Volume: Set the handset receiver volume.
Speakerphone Ring Volume: Set the ringtone volume in hands-free mode.
Handset SignalTone Volume: Set the volume for tones such as incoming and outgoing call signals.
Speakerphone SignalTone Volume: Set the hands-free call volume.

Alert Info Ring Setting

Alert-Info:
Access the webpage **[Phone Settings] >> [Media Settings] >> [Alert Info Ring Settings]** to configure Alert Info rules.
Parameters:

Alert-Info	
Values from Alert Info 1 to Alert Info 10	Set the values for specific ringtone types for incoming calls. When the device receives an Invite message with an Alert Info field value that matches the set value, the device will play the corresponding ringtone type.
Line	Set whether to enable specific ringtones for incoming calls on the respective SIP line.
Ring Type	Type1-Type7, WirelessRing

Tone Settings

Users can configure call tones, conversation tones, ringback tones, and hang-up reminder tones via the webpage **[Phone Settings] >> [Features] >> [Tone Settings]**.

Parameters	Description
Enable Holding Tone	There will be an alert tone when the user presses the hold call button during a call. This feature is enabled by default on the device.
Enable Call Waiting Tone	There will be an alert tone when a second incoming call is received during an ongoing call. This feature is enabled by default on the device.
Play Dialing 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.
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.
Play Boot Up Tone	The tone played when the device powers on and starts up.
Auto Answer Tone	**Enabled:** When there is an incoming SIP or IP direct dialing call, if automatic answering is enabled, there will be a prompt tone during the automatic answering. **Disabled:** When there is an incoming SIP or IP direct dialing call, if automatic answering is enabled, there will be no prompt tone during the automatic answering.
Ring Back Tone	**Closed**: Disables the ringback tone for calls. **Default**: Uses the default ringback tone. Supports custom ringback tones, which can be set by upgrading ringtone files under **[System] >> [Upgrade] >> [Ring Upgrade]**, and then selecting the custom option for the ringback tone.
Busy Tone	**Closed**: Disables the call waiting tone. **Default**: Uses the default call waiting tone. Supports custom call waiting tones, which can be set by upgrading ringtone files under **[System] >> [Upgrade] >> [Ring Upgrade],** and then selecting the custom option for the call waiting tone.

Upload Ring

Users can upgrade the ringtone by accessing the device webpage >> **[System] >> [Upgrade] >> [Ring Upgrade]**, selecting the ringtone file, and clicking **[Upload]**.

Ringtone file format:
Supports WAV
Maximum file size: 1 MB per file

Function Key Settings

Function Key

Function Key Setting

Users can configure function keys through the web management interface.

Web Interface Configuration of Feature Keys:

In the webpage **[Function Key]**, configure the DSSKEY keys. The key types can be memory keys, function keys, DTMF, etc. Assign the configuration to the corresponding device and update it.

Function Key Usage:

Function keys support the following types:

Memory Key

Voice Mail: In standby mode, press the key to play the voicemail.

Speed Dial: In standby mode, press the key to quickly dial a preset number.

Intercom: Make a call to the preset number via intercom. If the other party is set to receive intercom calls, they can automatically answer the intercom call.

Key Event

Voice Mail: In standby mode, press the key to play the voicemail.

Do-not-disturb: Enter the Do Not Disturb settings interface to enable/disable the Do Not Disturb feature.

Call hold: Hold/Resume current call.

Intercom: Open the dial pad and make a call to the entered number via intercom.

Prefix: Configure the number prefix. When dialing, press this key to automatically add the prefix number.

End: Press the key to end the current call.

Disposition: This feature relies on the Broadsoft server and is a method of recording call information in a call center.

Handfree: Enter hands-free dialing or switch to hands-free mode.

Answer Key: Press the key to answer the incoming call.

Private Hold: This feature is related to the Broadsoft server. During a call, if you don't want others to retrieve the call, you can use the Private Hold key.

DTMF: Press this key during a call to send the configured values in sequence to the remote end.

URL: Access the configured remote URL address, where you can set the XML phonebook address and more.

Action URL: Users can use a specific URL to perform basic call operations and configure multicast listening by setting the multicast address. When RTP is available, pressing the key allows listening to the multicast.

XML Browser: Place the configured XML file on an HTTP/HTTPS server. Press this key to retrieve the XML content and perform the corresponding action based on the content.

MCAST Listening: Configure the multicast listening function key on the function key page. After configuring the multicast address and port, save the settings. In standby mode, press the configured function key to listen to the multicast when the key is pressed.

Network Settings

Ethernet Connection

Users can configure the wired network through the device's web interface. The device defaults to IPv4 mode, and the Network Mode can be modified as needed.

Configure the wired network through the web interface:
Users can navigate to **[Network] >> [Basic] >> [IPv4 Settings]** on the web interface to configure the network type. Both Static IP and DHCP options 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.

Wireless Network (Only i501W)

The device supports wireless Internet capabilities. There are two ways to connect to Wi-Fi:
Go to the device web page **[Network] >> [Wi-Fi Settings]** to configure the wireless network connection.

- Use the built-in SSID and password, the same as W611W, and enable the **[Share Wi-Fi]** feature on W611W. Alternatively, change the AP's SSID and password to match i501W. After powering on, the device will automatically connect to the wireless network, provided it has been restored to factory settings and has no previously connected Wi-Fi networks.

To connect via the web interface:
Log in to the device web page, go to **[Network] >> [Wi-Fi Settings]**, and enable Wi-Fi.
After adding Wi-Fi information, click **[Add]**.
You will then see the connected Wi-Fi in the wireless network list.

To connect via another device (built-in default Wi-Fi SSID):
Method 1:

- Enable **[Share Wi-Fi]** on W611W: Go to Menu >> Advanced Settings >> 7. Share Wi-Fi. Turn on the Wi-Fi sharing feature and configure the SSID and password for the office network. At this point, the W611W functions as an AP.
- Power on the i501W device.
- After powering on, the W611W will push the office network's SSID and password to the i501W, enabling it to connect to the office network. When the Wi-Fi connection is successful, the power indicator will flash red five times quickly.

Method 2:

The user creates a Wi-Fi network with the SSID WiFi-device-ssid and password i<0%aY8+.
After powering on, the i501W device automatically connects to this Wi-Fi.
Upon successful connection, the power indicator will flash red quickly five times. The Wi-Fi information of the i501W can then be updated to connect to the office network using automatic deployment.
The Wi-Fi module configuration file is as follows:

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

<NET CONFIG MODULE>

--WIFI List--      :
Item1 WIFI Name         :WiFi-test
Item1 WIFI SSID        :WiFi-test
Item1 Secure Mode       :1
Item1 WIFI Encryption   :1
Item1 WIFI User Name     :
Item1 WIFI Password     :12345678

<<END OF FILE>>
```

Network Mode

There are three IP Mode options available: IPv4, IPv6, and IPv4 & IPv6.
Users can also set the network mode via the web interface by going to **[Network] >> [Basic] >> [Network Type].**

Network Server

Setting Method:
Log in to the device web page **[Network] >> [Service Ports] >> [Server Port Settings]** to configure the web server type, which allows configuration of web login protocol type, login ports, and other parameters.

Configuration Details:
Web Server Type: Changes take effect after a restart. You can choose the web login to be either HTTP or HTTPS.
Web Login 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 1025-65530, and the RTP port value starts from the configured initial value; with each call, the voice and video port values increase by 2.

RTP Port Quantity: The number of calls.

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 Manager webpage **>> [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.

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

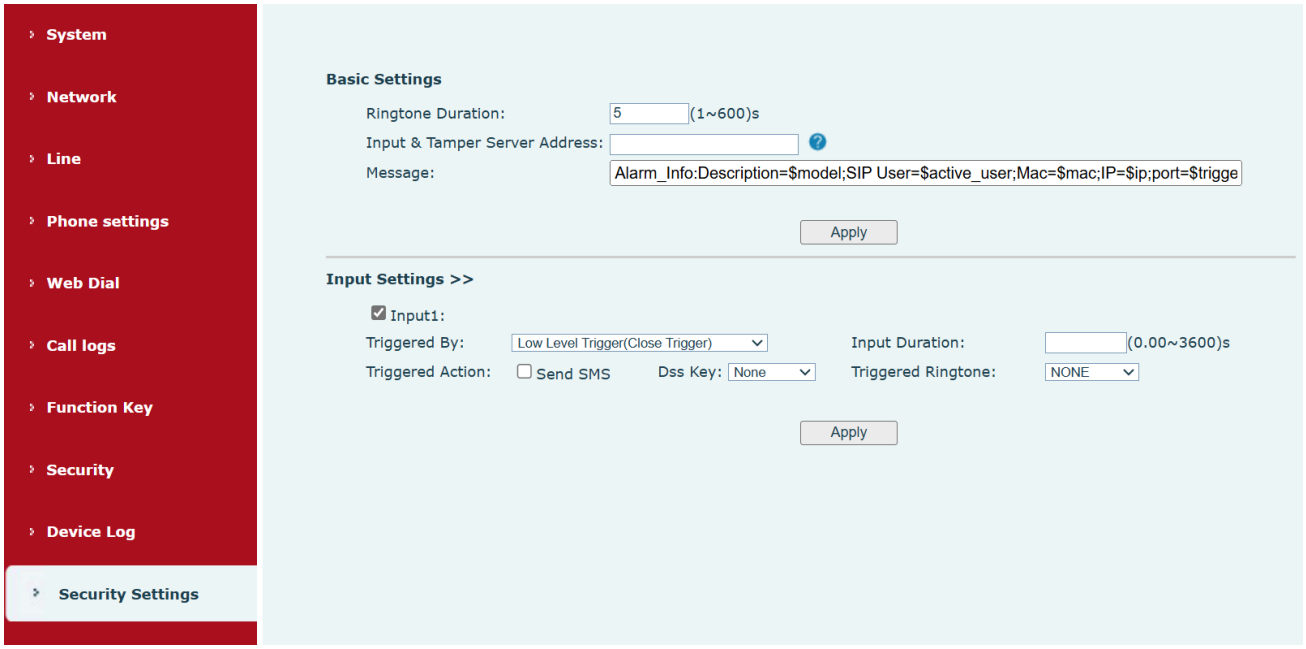
DHCP VLAN
Access the device web page **>> [Network] >> [Advanced] >>** DHCP VLAN Settings, configure DHCP VLAN parameters:
Selection of Option Value: Enable or disable acquiring the VLAN ID through DHCP OPTION.
DHCP Option VLAN: Set the OPTION value, 128-254, to obtain the VLAN value via DHCP.

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.

Security Settings

Short-circuit Input

Short-circuit input detection interface: Used for connecting devices such as switches, infrared probes, door sensors, and vibration sensors;
When the short-circuit input is triggered, it can send a text message to a specified server address, or make a call to a designated number, and play an alarm ringtone locally. This facilitates quick response by management personnel.
Users can configure security information on this interface. When the device is triggered according to the alarm information, it will send an alarm message to the server and play the preset alarm ringtone.



Parameters	Description
Basic Settings	
Ringtone Duration	When the input interface triggers an alarm, if the alarm sound is enabled, specify the duration of the alarm sound.
Input & Tamper Server Address	Configure the remote response server address, including the remote response server address and the triggered alarm server address. When the input interface or tamper is triggered, it will send a short message to the server. The server address supports IP:PORT or SIP number.
Information	The alarm information to be sent: The $parameter can be replaced with actual values. The supported parameters are as follows: $model: Replaced with the actual model name. $active_user: Replaced with the actual SIP username. $mac: Replaced with the device's MAC address. $ip: Replaced with the device's IP address. $trigger: Replaced with the triggered interface, such as input1,

	input2, etc. $triggerName: Replaced with the name of the trigger.
Input settings	
Parameters	**Description**
Input 1	Enable or disable Input 1
Triggered by	When choosing the low level trigger (closed trigger), detect the input port (low level) closed trigger.
	When choosing the high level trigger (disconnect trigger), detect the input port (high level) disconnected trigger.
Input Duration	Set the Input change duration time, the default is 0 seconds.
Triggered Behavior	Enable or disable the input port from sending messages to the server.
DSS Key	Select the DSSKey to configure.
Triggered Ringtone	Supports ringtone selection: None, no ringtone triggered.

Security

Web Password

Modify the password through the user configuration interface:
Users can customize and change the web login password by accessing the webpage at **[System] >> [Account] >> [User Management]** and selecting the account to modify.

Modify the password by logging into the user interface:
Users can customize and change the web login password. After logging into the webpage, click on Default password is in use. Please change in the upper right corner to modify it.

Password change settings:
Current Password: Enter the web login password.
New Password: Enter the new login password.
Confirm Password: Re-enter the new login password to confirm.

Note:
After changing the password, you will be automatically logged out and must re-enter the new password to log in again.

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 webpage **[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 **[Submit]** 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.

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.

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.

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 three types of filtering protocols: TCP | UDP | ICMP.
Src Port Range	Filter port range
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.

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.

Get Device System Information

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

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

Reboot Device

Users can restart the device via the web interface.

Web Interface Restart:
Click on **[System] >> [Reboot Device] and press [OK].**

Power Cycle Restart:
Simply unplug the device and plug it back in to restart.

Device Factory Reset

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

Web Interface Restore:
Click on **[System] >> [Configurations] >> [Reset Device] >> [Reset] button and press [OK]**.

Network Packets Capture

In order to obtain the data packet of the device, the user needs to log in to the webpage of the device, open the webpage **[System] >> [Tools] >> [LAN Packet Capture]**, and click the **[Start]** option in the "Network Packets Capture".If you are using a WiFi 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 webpage 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.

Get Device Log

When encountering abnormal issues, log information can be helpful. The device supports exporting

system logs and WiFi logs.

Obtain system log:
To obtain the device's log information, users can log into the device's webpage, 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 WiFi 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.

Common Trouble Cases

Trouble Case	Solution
Device could not boot up	The device is powered by a power adapter. Please use a compliant power adapter and check if the device is connected to power. The device is powered by PoE. Please use a compliant PoE switch.
Device could not register to a service provider	Please check if the device is connected to the network  . 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. 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 "16.5 Network Data Capture" to obtain network packets for analysis. Send them to the support email to help diagnose the issue.

Appendix Table

Appendix I - Button Icon

Icon	Description
	Management Office
	Do Not Disturb
	Hands-free Call
	Door Open