i60&i60K
User Manual

Version: T2.12 | Date: 2024.8.1

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 i60 and i60K are newly designed SIP audio and video intercoms from Fanvil. The products feature an all-aluminum alloy construction with an explosion-proof rating of IK07. The sleek and well-defined lines not only provide a luxurious and elegant appearance but also ensure robust protection. They support multiple door opening methods and use the standard SIP protocol, offering high-definition voice communication quality. These devices provide users with premium access control security and intercom services.

2.2 Specification Parameter

参数/型号	i60	i60K
产品工艺	ABS+PC	ABS+PC
外观尺寸（L*H*W)	50*130*30mm（不含防雨罩）	70.7*149.7*30mm（不含防雨罩）
按键	单一呼叫按钮	1 个呼叫按钮+数字键盘
摄像头	200W 像素	
图像传感器	1/2.9”	
SIP	2 条线路	
视频	H.264	
语音	高清语音 G.722/Opus	
供电方式	DC12V/POE	
有线网络	单网口百兆	
验证方式	IC 卡开门、蓝牙、远程开门	密码开门、IC 卡开门、蓝牙、远程开门
数据传输接口	韦根输入/输出*1、继电器输出*1、短路输入*2	
防拆报警	支持	
IP 等级	IP65	
工作温度	-20°C～+60°C	
存储温度	-30°C～+70°C	
安装方式	壁挂、防雨罩	
适用环境	室内、室外	

3 Appearance Overview

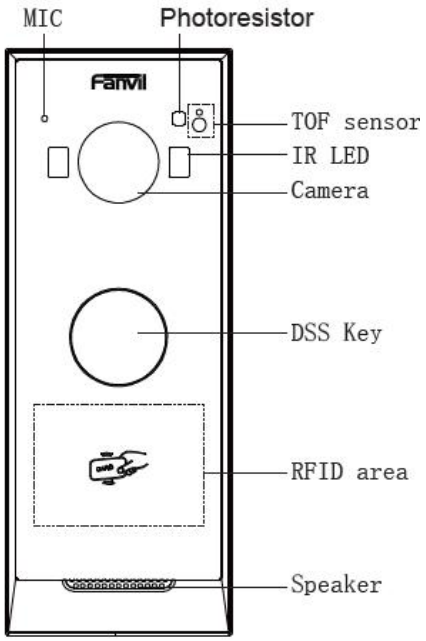
3.1 i60 Appearance

Six Views of the Product -i60

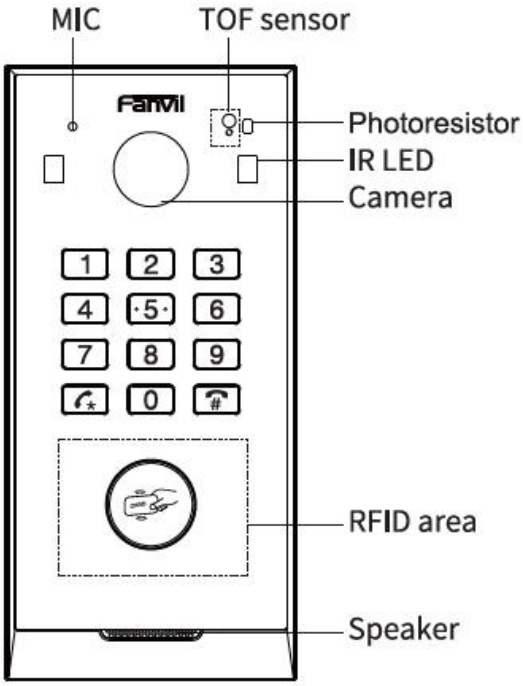
3.2 i60K Appearance

Six Views of the Product -i60K

3.3 i60 Panel Overview



3.4 i60K Panel Overview



4 Installation Instruction

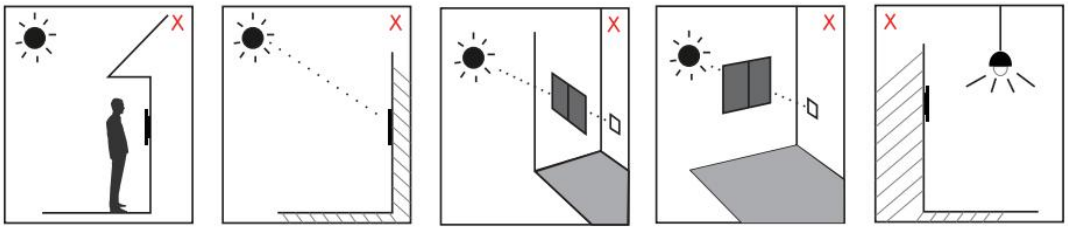
4.1 Product Installation Instruction

Step 1: Installation Environment

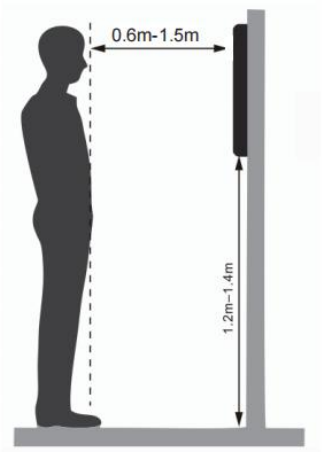
4.1.1 Installation Environment

- Do not install the device in the following locations: direct sunlight, high temperatures, low temperatures, corrosive chemicals, or excessive dust. Install the device at an appropriate visual height, with a recommended height of approximately 120-140 cm.
- If installing indoors, maintain at least 2 meters away from light sources and at least 3 meters away from doors and windows to avoid direct sunlight.
- Avoid severe vibrations, collisions, and impacts, as they may damage internal precision components and the exterior casing.

  If any issues arise when powering on the device, immediately cut off the power and resolve the problem. Follow the user manual for inspection after abnormal disconnection. Contact the sales agent or manufacturer for unresolved issues and avoid self-repair. Keep access cards safe from magnetic fields, water, or bending. For facial recognition models, install in evenly lit environments, avoiding strong backlight, oblique light, or close-range illumination.



Backlighting | Direct sunlight | Direct sunlight through windows | Angled sunlight through windows | Too close to the light source



4.1.2 Device Inventory

NO.	Name	Quantity	Notes
1	Device	1	i60 or i60K Device Body
2	Wall Bracket	1	Mounting Bracket for the Device; Choose either the wall mount bracket or the rain cover for installation.
3	Rain Cover	1	
4	7-Pin Connecting Cable	1	Short-circuit Input, Wiegand Interface Cable
5	5-Pin Connecting Cable	1	Power Supply, Normally Open, Normally Closed
6	Cable Outlet Cover and Gasket	1	After connecting the wires, install the cable outlet cover for waterproofing.
7	KA4*25 Phillips Screw	4	Screws for Installing Wall Mount Bracket or Rain Cover
8	φ6*30mm Rubber Plug	4	Rubber Plugs for KA425 Screws Installation
9	KM3*5 Phillips Screw	2	Screws for Securing the Device to the Bracket
10	KM2*6 Phillips Screw	6	Screws for Securing the Cable Outlet Cover

4.1.3 Installation Tool Preparation

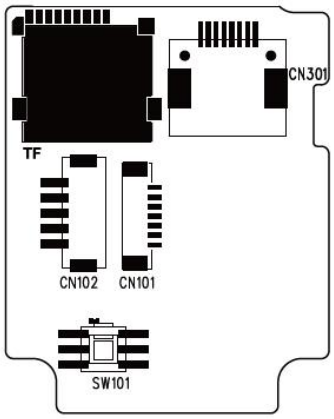
NO.	Name	Specifications
1	Phillips Screwdriver	Ph2 or Ph3, preferably magnetic
2	Impact Drill	Recommended: 850W Impact Drill
3	Drill Bit	8mm Impact Drill Bit
4	RJ45 Crimping Tool	/
5	Others	Network Cables, RJ45 Connectors, Electrical Tape, or Terminal Blocks (as needed)

4.1.4 Product Installation

1. Use the installation dimensions diagram to mark the positions of the installation holes on the wall.
2. Before marking the installation holes, use a level or another method to verify that the dimensions diagram is horizontally aligned to ensure the device is installed vertically.
3. Use an impact drill to drill holes at the marked positions, ensuring the depth of the holes is 2 cm.
4. Use a hammer to insert φ6*30mm wall plugs into the drilled holes until they are flush with the wall.
5. Place the mounting bracket over the drilled holes, ensuring the holes on the bracket align with the wall plugs.
6. Use KA4*25 screws to secure the bracket to the wall, tightening them with a screwdriver.
7. Take out the device, connect the network cable and other wires to the corresponding positions on the device, and install the cable cover using KM2*6 cross screws. Be sure to place the gasket in the cable cover. If the cable outlet is too small, you can use pliers to adjust the cable opening.
8. Place the device onto the mounting bracket or rain cover from bottom to top, and secure it at the bottom of the device using KM3*5 screws.

4.2 Terminal Connection and Terminal Description

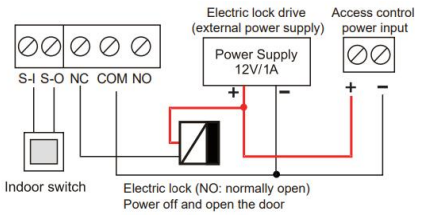
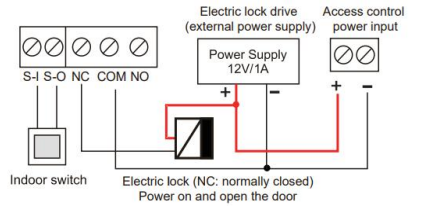
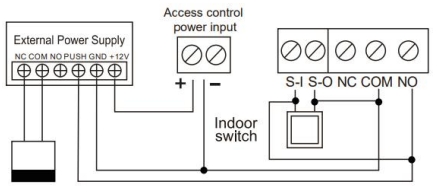
The i60 & i60K terminal connections and descriptions are shown below:



Terminal Block	Name	Color	Description
CN101	DOORA	Red	Two sets of short-circuit input detection interfaces: used for connecting switches, infrared sensors, door magnets, vibration sensors, and other input devices.
	GND	Black	
	DOORB	Brown	
	GND	Black	
	WG_D1	Yellow	Wiegand interface (D0/D1/GND)
	WG_D0	White	
	GND	Black	
CN102	12V+	Red	12V DC input interface
	GND	Black	
	NC	Yellow	Normally open/normally closed control interface: used for controlling electric locks, alarms, and other devices.
	COM	Green	
	NO	White	
CN301	Ethernet	/	Standard RJ45 interface, 10/100M auto-sensing. It is recommended to use Cat5 or Cat5e Ethernet cables.
SW101	Tamper Switch	/	Tamper switch
TF	TF Card Slot	/	TF card installation location

4.3 Wiring Instruction

NO: Normally Open Contact
COM: Common Contact
NC: Normally Close Contact

Driving Mode	Electric-lock Mode		Connections
Passive	No electricity when open	Electricity when open	
√	√		
√		√	
√	√		

Note:

1. For DC power, indoor switches, and door lock cables, it is recommended to use RVV2*0.5.
2. For network cables, it is recommended to use Cat5, Cat5e, or Cat6 cables. Cat6a cables may not connect properly to the device.

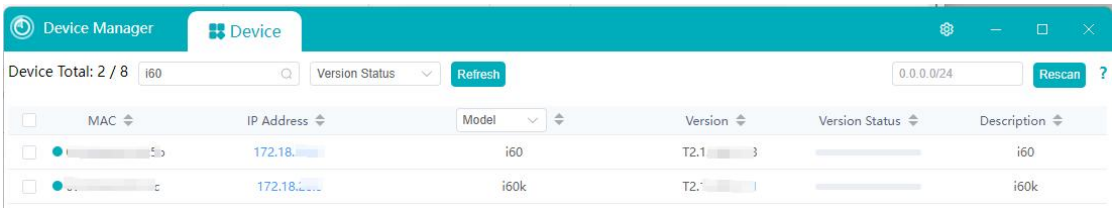
5 Device Configuration

5.1 Log in to the Product Management Interface

5.1.1 Searching Door Phone

Method 1: Obtain Device IP using a Scanning Tool:

1. Connect the computer and i60/i60K to the same local network and install Device Manager on the PC.
2. Open the IP scanning tool (Device Manager), and click "Scan" to obtain the IP address of the i60/i60K devices on the local network.



Method 2:

1. Press and hold the speed dial key for 3 seconds (after 30 seconds of power-on). When you hear a prompt sound, press the speed dial key again to hear the IP address announced.
2. Additionally, the device provides a way to switch the IP address retrieval method via the surface speed dial key:
3. Hold the speed dial key for 3 seconds. When the speaker beeps rapidly, press the key three times within 5 seconds to hear the new IP address.

5.1.2 Log In to the Device Web Interface

1. Use a web browser to enter the device's IP address to access the management interface. The default username is admin and the password is admin. It is recommended to change the username and password immediately after logging in.
2. When logging into the management interface, you can select the interface language.

Note:

Users must provide the correct username and password to log in to the management interface. If the password is entered incorrectly three times, the account will be locked

and can only be accessed again after 5 minutes.

Specific details are as follows:

(1) If a single IP address attempts to log in with different usernames more than the specified number of times, it will be locked.

(2) If a single username is used to log in from different IP addresses more than the specified number of times, it will also be locked.

5.1.3 快速入门

设备可在本地单独使用也可以配合 FCMS 使用，以下介绍 2 种方式的快速入门设置。

■ **本地使用**

登录设备后，首先进行网络设置，设备连接网络后，进行线路设置、快捷键设置和门禁设置，详情可参照 5.3、5.4、5.7、5.11。

■ **配合 FCMS 使用**

登录设备后，设备连接网络后，在 5.11 中设置完成继电器、开门方式等门禁规则后，即可在 FCMS 平台注册设备、授权用户等相关操作。

5.2 System

5.2.1 Information

Users can view the device's system information, including model, hardware version, software version, uptime, last boot time, memory information, system time, network information, and SIP account status.

5.2.2 Account

Users can change the password for logging into the web interface. Users with admin privileges can also add or delete users, manage users, and set permissions and passwords for new users.

5.2.3 Configurations

Users with admin privileges can view, export, or import device configurations on this

page, and can also restore the device to factory settings.

- **Export Configurations**

  Right-click and select "Save As" to download the device's configuration file, with a .txt extension. (**Note: Exporting configuration files requires admin privileges**)

- **Import Configurations**

  Import a previously saved configuration file.

- **Clear Configuration**

  Select the modules you want to clear from the configuration file:

  SIP: Account-related configuration

  AUTOPROVISION: Auto-upgrade related configuration

  TR069: TR069-related configuration

  MMI: MMI module, including user authentication information, web access protocols, etc.

  DSSkey: DSSkey configuration

  Basic Network: Basic network settings

- **Clear Tables**

  Select the local data tables to clear (default is to select all).

- **Reset Phone**

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

5.2.4 Upgrade

Local Upgrade:

Upgrade the device software version by using the web interface to update to a new version. After the upgrade is complete, the device will automatically restart to apply the new version. Click "Select," choose the version, and then click "Upgrade" to proceed

Upgrade ringtone files, supporting WAV and MP3 formats.

Online Upgrade:

The firmware online upgrade involves the device sending an HTTP request to the server. The server returns the corresponding description file or a 404/error timeout. The device then parses the version description file and prompts the user with the new version information, asking if they want to upgrade.

Parameters	Description

Upgrade Server	
Upgrade Server Address 1	Enter the address of the primary upgrade server (HTTP server).
Upgrade Server Address 2	Enter the address of the backup upgrade server (HTTP server). The backup server will be used if the primary server is unavailable.
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 the server has the corresponding TXT file and version, the [Upgrade] button becomes active from a disabled state. Clicking [Upgrade] allows you to choose whether to proceed with the upgrade.
New Version Description	When the server has the corresponding TXT file and version, the new version description information will display the version information from the TXT file.

- The file requested by the device from the server is a TXT file named vendor_model_hw1_0.txt. 'hw' represents the hardware version number. Any spaces in the file name should be replaced with underscores.
- The URL requested by the device is HTTP://server_address/. Both the new version and the requested file must be placed in the download directory of the HTTP server.
- The TXT file format must be UTF-8.
- vendor_model_hw1_0.txt file format reference is as follows:

  Version=1.6.3 # software version

  Firmware=xxx/xxx.z #xxx.z or http:// server_address IP: port/directory/xxx.z

  BuildTime=2024.08.11 20:00

  Info=TXT|XML

  Xxxxx

  Xxxxx

  Xxxxx

  Xxxxx

5.2.5 Auto Provision

The terminal supports four methods for automatic deployment: SIP Plug-and-Play, DHCP Option Parameters, Static Deployment Server, and TR069.

Supported transmission protocols include: FTP, TFTP, HTTP, and HTTPS.

Auto Provision	
Parameters	**Description**
Basic Settings	
CPE Serial Number	Displays the current device serial number.
Authentication Name	Configures the username for the FTP server; not required for TFTP protocol; if using FTP protocol for download, and this field is left blank, the default FTP user will be anonymous.
Authentication Password	Configures the password corresponding to the FTP server username.
Configuration File Encryption Key	If the configuration file to be upgraded is encrypted, enter the encryption password for the configuration here.
General Configuration File Encryption Key	If the generic configuration file to be upgraded is encrypted, enter the encryption password for the configuration here.
Save Auto Provision Information	Configures whether to save automatic update information.
Download CommonConfig Enabled	Determines whether to download the generic configuration file during automatic upgrade.

Enable Server Digest	If the terminal uses Digest authentication to match configuration file content, the terminal will update and download if the configuration on the server changes or does not match the terminal configuration.
DHCP Option	
Option Value	Configures DHCP option. DHCP option supports DHCP custom option, DHCP option 66, and DHCP option 43 for obtaining automatic deployment application parameters. When obtaining parameters via DHCP, the user can choose any one of these; by default, the terminal is set to disable DHCP option.
Custom Option Value	Custom option valid values range from 128 to 254. The custom option type must match the definition provided by the DHCP server.
Enable DHCP Option 120	Configures SIP server address using DHCP option 120.
DHCPv6 Option	
Option Value	Configures DHCP option. DHCP option supports DHCP custom option, DHCP option 66, and DHCP option 43 for obtaining automatic deployment application parameters. When obtaining parameters via DHCP, the user can choose any one of these; by default, the terminal is set to DHCP option 66.
Custom Option Value	Custom option valid values range from 128 to 254. The custom option type must match the definition provided by the DHCP server.
Enable DHCP Option 120	Configures SIP server address using DHCP option 120.
SIP Plug And Play (PnP)	
Enable SIP PnP	Configures whether to enable PnP. If PnP mode is enabled, the terminal will periodically send SIP SUBSCRIBE messages in multicast mode after startup. Any SIP server supporting this specific message will respond with a SIP NOTIFY message containing the automatic configuration/deployment server path, allowing the terminal to obtain the configuration file to download.
Server Address	Configures the PnP server.

Server Port	Configures the PnP port.
Transport Protocol	Configures the PnP transmission protocol.
Update Interval	Configures the PnP timeout period, in hours.
Static Provisioning Server	
Server Address	Configures the FTP server address. The server address can be in IP form (e.g., 192.168.1.1) or domain name form (e.g., ftp.domain.com). The system also supports server subdirectory settings, such as 192.168.1.1/ftp/Config/ or ftp.domain.com/ftp/config, meaning the server address is 192.168.1.1 or ftp.domain.com, and the file path is /ftp/Config/. Subdirectory paths can end with or without a “/”.
Configuration File Name	Configures the name of the configuration file to be upgraded. Typically, this field is left empty for automatic upgrades, allowing the device to use its MAC address as the file name to fetch the file from the server.
Protocol Type	Selects the server type, which can be FTP, TFTP, or HTTP.
Update Interval	Configures the interval for updates, in hours.
Update Mode	Types of automatic updates 1. No update 2. Upgrade after reboot 3. Interval update, which updates periodically
Autoprovision Now	
TR069	
Enable TR069	Configures whether to enable TR069.
ACS Server Type	Selects the ACS server type; currently supports telecom and standard ACS servers.
ACS Server URL	Enter the ACS server address.
ACS User	Enter the ACS server authentication username.
ACS Password	Enter the ACS server authentication password.
Enable TR069	Configures whether to enable TR069 prompt tone.

Warning Tone	
TLS Version	If auto-login is selected, the device will not prompt for a username and password upon restart but will use the previously entered correct username and password to connect to the ACS server.
INFORM Sending Period	Configures the interval for sending notifications, in seconds. Valid range: 1 to 999999.
STUN Server Address	Enter the STUN address.
STUN Enable	Configures whether to enable STUN.

5.2.6 Tools

Provides tools for users to resolve issues. For example, you can set the address of the syslog software. During operation, the device's log information will be recorded in the syslog software. If problems arise, you can send the log information to the device manufacturer’s technical support for analysis.

5.2.7 Reboot

Allows you to restart the device.

5.3 Network

5.3.1 Basic

Users can configure network connection types and parameters through this page.

Parameters	Description
Network Mode	IPv4、IPv6、IPv4&IPv6
IPv4 Network Status	
IP	Current device IP
Subnet Mask	Subnet mask

Default Gateway	Current preset gateway IP
MAC	Displays the device's MAC address
IPv4 Settings	
The device's network connection method should be selected based on the actual network environment. The device offers three network modes:	
Static IP	If your ISP provides a fixed IP address, select this option. You must enter the static IP address, subnet mask, gateway, and DNS information. If you don't have this information, contact your ISP or network administrator for assistance.
DHCP	When this mode is selected, network information is automatically obtained from the DHCP server, so you do not need to manually enter these fields.
PPPoE	When this mode is selected, you must enter the ADSL login account and password.
Enable Vendor Identifier	When enabled, the vendor identifier will be visible in the DHCP option 60 field.
Vendor Identifier	Supports customization; when vendor identification is enabled, the vendor identifier will be visible in the DHCP option 60 field.
When using the static mode, you need to configure the relevant static settings.	
DNS Server Configured by	Select the DNS server configuration mode
Primary DNS Server	Enter your primary DNS server address
Secondary DNS Server	Enter your secondary DNS server address
DNS Domain	Enter your DNS domain name
Note: 1. After setting the parameters, click **[Apply]** to apply the changes. 2. If you change the IP address, the web page will no longer respond. You need to enter the new IP address in the address bar to reconnect to the device.	

5.3.2 Service Port

This page provides settings for web login protocols, protocol ports, and RTP ports.

Parameters	Description
Web Server Type	The settings will take effect after a restart. You can choose between HTTP/HTTPS for web login.
Web Logon Timeout	The default timeout is 15 minutes, after which the login page will automatically log out, and you will need to log in again.
Web Auto Login	After timeout, you won't need to enter the username and password; it will auto-login.
HTTP Port	The default port is 80. For better security, you can set a port other than 80, such as 8080. Web login would then be: HTTP://ip:8080.
HTTPS Port	The default port for HTTPS is 443, used similarly to the HTTP port.
RTP Port Range Start	The valid range for RTP port values is 1025-65535. The RTP port value increments by 2 for each call, for both voice and video.
RTP Port Quantity	Number of calls made.

5.3.3 VPN

Virtual Private Network (VPN) is a technology that allows a device to create a connection to a server and become part of the server's network. The device's network traffic can be routed through the VPN server.

For some users, particularly enterprise users, a VPN connection may need to be established before activating line registration. The device supports two VPN modes: Layer 2 Tunneling Protocol (L2TP) and OpenVPN protocol.

Users must enable (or disable) and configure the VPN by logging into the web interface.

- **L2TP**

Note: The device only supports basic, unencrypted authentication and data transmission.

If users require data encryption, please use the OpenVPN feature instead.

Users must log into the device's web interface and navigate to **Network** >> **VPN** to establish an L2TP connection. In VPN mode, check the "Enable VPN" option, select "L2TP," and then fill in the L2TP server address, L2TP authentication username, and password. Click "Apply," and the device will attempt to connect to the L2TP server.

When establishing a VPN connection, the VPN IP address will be displayed in the VPN status section. There may be delays in establishing the connection. Users need to refresh the page to update the status in a timely manner.

Once VPN configuration is successful, the device will automatically attempt to connect to the VPN each time it starts, as long as the VPN is not disabled. If the VPN connection is not established promptly, users can try restarting the device and then check if the VPN connection is successfully established.

■ **OpenVPN**

To establish an OpenVPN connection, users receive authentication and configuration files from the OpenVPN service provider. The names of these files are as follows:

OpenVPN Configuration file: client.ovpn

CA Root Certification: ca.crt

Client Certification: client.crt

Client Key: client.key

Then, users upload these files to the device's web interface under **Network** >> **VPN**, and select the OpenVPN files. Users need to check the "Enable VPN" option, select "OpenVPN" in the VPN mode, and finally check "Apply" to enable the OpenVPN feature. Similar to the L2TP connection method, the system will establish the OpenVPN connection automatically each time it restarts, until the user manually disables it.

5.3.4 Advanced

Advanced network settings are typically configured by IT administrators to enhance the quality of device services.

Parameters	Description
LLDP Settings	
Enable LLDP	Enable Link Layer Discovery Protocol (LLDP) for

	network discovery.
Packet Interval	Set the interval for LLDP packets to be sent.
Enable Learning Function	Learn and store information about discovered devices on the device.
Enable CDP	Enable Cisco Discovery Protocol (CDP), set the interval for CDP packets to be sent.
QoS Settings	
Enable DSCP	Voice Quality Assurance (default disabled)
DHCP VLAN Settings	
DHCP Option VLAN	128-254, obtain VLAN values via DHCP
WAN VLAN Settings	
Enable VLAN	WAN Port Settings
802.1X Settings	
802.1x Mode	Authenticate network clients (or ports)
Identity	Authentication Username
Password	Authentication Password

5.4 Line

5.4.1 SIP

Configure SIP information on this page. The configuration details are as follows:

Configure SIP information on this page. The configuration details are as follows

Parameters	Description
Register Settings	
Line Status	It displays the current status of the line. To obtain the latest online status, users must manually refresh the page.
Activate	The service for this line is enabled.
Username	Enter the username for the service account.
Authentication User	Enter the authentication name for the service account.
Display name	Enter the name displayed when the call request is sent.

Authentication Password	Enter the authentication password for the service account.
Realm	Enter the SIP domain provided by the service provider.
Server Name	Enter the server name.
SIP Server 1	
Server Address	Enter the SIP server address.
Server Port	Enter the SIP server port.
Transport Protocol	Set the SIP transport line to use TCP, UDP, or TLS.
Registration Expiration	Set the SIP expiration time.
SIP Server 2	
Server Address	Enter the SIP server address.
Server Port	Enter the SIP server port.
Transport Protocol	Set the SIP transport line to use TCP, UDP, or TLS.
Registration Expiration	Set the SIP expiration time.
Proxy Server Address	Enter the IP address of the SIP proxy server.
Proxy Server Port	Enter the port of the SIP proxy server, default is 5060.
Proxy User	Enter the proxy username.
Proxy Password	Enter the proxy password.
Backup Proxy Server Address	Enter the backup proxy server address.
Backup Proxy Server Port	Enter the backup proxy server port, default is 5060.
Basic Settings	
Enable Auto Answering	Enable auto-answer, which will automatically answer calls after the delay time has passed.
Auto Answering Delay	Set the system's auto-answer wait time.
Enable Hotline	Enable hotline configuration. When activated, the voice

	channel device will dial the configured number.
Hotline Delay	Set the delay time for dialing the hotline number.
Hotline Number	Set the hotline dialing number.
Dial Without Registered	Allow outgoing calls without registration.
DTMF Type	Set the DTMF type for the line.
DTMF SIP INFO Mode	Set the SIP INFO mode to send '*' and '#' or '10' and '11'.
Request With Port	The URI may or may not carry port information.
Use VPN	Set the line to use the VPN network.
Use STUN	Ensure NAT traversal settings use STUN for the line.
Enable Failback	Switch to the primary server when it is available.
Failback Interval	Set the interval for periodically probing the availability of the primary proxy using Register messages.
Signal Failback	In the case of multiple proxies, allow invite/register requests to also perform failback.
Signal Retry Counts	Number of attempts to consider a proxy unavailable in the case of multiple proxies for SIP requests.
Codecs Settings	Set the priority and availability of codecs by adding or removing them from the list.
Advanced Settings	
Use Feature Code	If this setting is enabled, the functions in this section will be controlled by the server instead of the device itself. To control the device, it will send feature codes to the server using the number specified in the dial code field.
Enable Blocking Anonymous Call	Dial feature codes to the server.
Disable Blocking Anonymous Call	Dial the feature codes to the server.
Call Waiting On Code	Dial feature codes to the server.

Call Waiting Off Code	Dial the feature codes to the server.
Send Anonymous On Code	Dial the feature codes to the server.
Send Anonymous Off Code	Dial the feature codes to the server.
Enable Session Timer	Enable call timing feature. If the call duration exceeds the timeout before receiving the call conference time, the call will be ended.
Session Timeout	Set the call timeout duration.
Response Single Codec	If enabled, the device will use a single codec to respond to incoming call requests.
BLF Server	In a standard BLF application, the device sends subscription packets to the registered server. If your server does not support subscription packets, please enter the BLF server. This will separate the registration server from the subscription server.
Keep Alive Type	Set the line to use UDP or SIP OPTIONS packets to ensure NAT is open.
Keep Alive Interval	Set the interval for sending keep-alive packets.
Keep Authentication	Retain previously validated authentication parameters.
Blocking Anonymous Call	Reject any incoming calls without caller ID.
User Agent	Set the user agent; by default, it matches the software version.
Specific Server Type	Work with specific server types. For details, refer to the "X5S/X6 Administrator User Manual."
SIP Version	Set the SIP version.
Anonymous Call Standard	Set the anonymous call standard.
Local Port	Set the local port.
Ring Type	Set the ringtone type for the line.
Enable user=phone	The user=phone field value is present in the INVITE SIP

	message.
Use Tel Call	Configure whether to enable the use of telephone calls.
Auto TCP	Configure to automatically use TCP protocol for transmission when the message body exceeds 1500 bytes; ensure the reliability of transmission.
Enable Rport	Configure the line to add the Rport SIP header.
Enable PRACK	Configure the line to support PRACK SIP messages.
DNS Mode	Choose the DNS mode: A, SRV, NAPTR.
Enable Long Contact	Configure the Contact field to carry additional parameters; use with the SEM server.
Enable Strict Proxy	Compatible with special servers (use the source address of the other party when returning messages, instead of using the address in the via field).
Convert URI	Configure whether to enable URI transformation.
Use Quote in Display Name	Specify whether to add a display name with quotation marks.
Enable GRUU	Configure to enable GRUU.
Sync Clock Time	Synchronize with server time.
Enable Use Inactive Hold	When enabled, the SDP in the INVITE packet will show "inactive" during call hold.
Caller ID Header	Configure the Caller ID header field.
Use 182 Response for Call waiting	Set the device to use a 182 Queued Response.
Enable Feature Sync	Enable/Disable Feature Sync
Enable SCA	Enable/Disable SCA (Shared Call Appearance)
CallPark Number	Set the caller ID forwarding number
Server Expire	Set the timeout to use the server's value
TLS Server Expire	Select TLS version
uaCSTA Server Expire	Set uaCSTA number

Enable Click To Talk	Used with special servers; enable this to allow direct dialing by clicking.
Enable ChangePort	Whether to enable port updates
Intercom Number	Set intercom number
Unregister On Boot	Whether to enable the logout function
Enable MAC Header	Whether to include the MAC address in the SIP package during registration
Enable Register MAC Header	Whether to include the MAC address in the User-Agent field during registration
PTime(ms)	Configure whether to include the ptime field; by default, it is not included.
Enable Deal 180	Enable: When receiving 183 + SDP, play IVR; if 180 is received afterward, play a local tone. Disable: When receiving 183 + SDP, play IVR; if 180 is received afterward, do not play a local tone.
SIP Global Settings	
Strict Branch	Set strict matching for the Branch field.
Enable Group	Enable group settings.
Enable RFC4475	Enable RFC4475.
Enable Strict UA Match	Enable strict UA matching.
Registration Failure Retry Time	Set the registration retry interval.
Local SIP Port	Modify the device's SIP port.
Enable uaCSTA	Enable the uaCSTA feature.

5.4.2 SIP Hostpot

SIP hotspot is a simple and practical feature. It is easy to configure and can extend the number of SIP accounts, achieving group ringing functionality.

Set up device A as the SIP hotspot and configure devices B and C as SIP hotspot clients.

When a call is made to device A, all devices (A, B, and C) will ring. Answering the call on any one of these devices will stop the ringing on the others, preventing simultaneous answering. When devices B or C make an outbound call, it will be made using the SIP number registered on device A.

Table 10 - SIP Hotspot Parameters

Parameters	Description
Enable Hotspot	Set the "Enable Hotspot" option in the SIP hotspot configuration to enabled.
Mode	This device can only be used as a client.
Monitor Type	The monitoring type can be either broadcast or multicast. If you want to limit broadcast packets on the network, you can choose multicast. The monitoring types on the server side and client side must be consistent. For example, if the client's device is set to multicast, the device serving as the SIP hotspot server must also be configured for multicast.
Monitor Address	When the monitoring type is multicast, the client and server use a multicast communication address. If broadcast is used, there is no need to configure this address; the system will default to using the broadcast address of the device's WAN port for communication.
Local Port	Enter the custom hotspot communication port. The port numbers on both the server and client must be consistent.
Name	Enter the name of the SIP hotspot. This configuration helps differentiate between different hotspots on the network to avoid connection conflicts.
Line Settings	Set whether to enable the SIP hotspot function on the respective SIP line.

When the device acts as a SIP hotspot client, there's no need to set up a SIP account; the device will automatically obtain and configure it upon activation. Just set the mode to "Client," and configure other options the same way as for the hotspot.

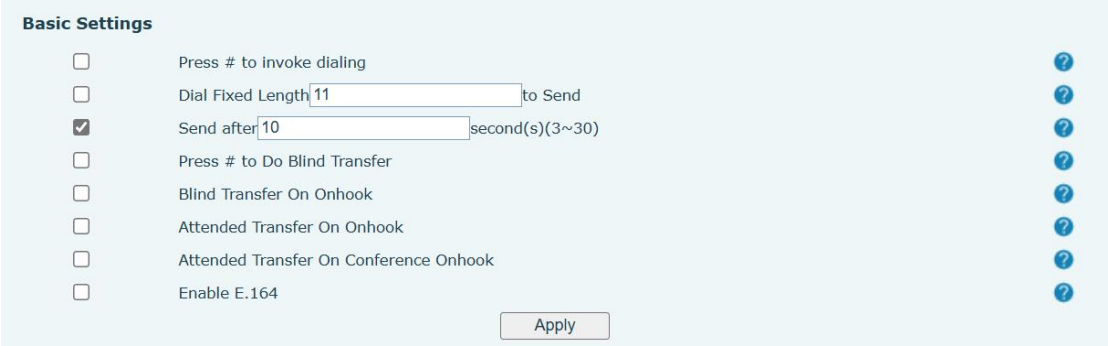
When the device functions as a hotspot server, the default extension number is 0. When the device functions as a client, extension numbers start from 1 and increment from there (you can view the extension numbers on the [SIP Hotspot] page of the web interface).

To call internal extension numbers:

- Hotspot servers and clients can dial each other using extension numbers.
- For example, extension 1 can call extension 0.

5.4.3 Dial Plan

Call number rules allow users to enable/disable existing rules or add custom dialing rules to achieve their desired dialing effects.



Parameters	Description
Press # to invoke dialing	Users can dial the number followed by the # symbol to initiate the call (supported only by i60K).
Dial Fixed Length to Send	The system automatically dials the number once the entered digits reach a fixed length.
Send after X second(s)(3~30)	The system automatically dials the number after a timeout period.
Enable E.164	Please refer to the **E.164 standard for specifications**.

Add dialing rules:

Parameters	Description
Dial Plan	To add outbound numbers, you can set them up in two ways: 1. Exact Match: The device will use the mapped IP address or configuration only if the dialed number matches exactly. 2. Prefix Match: This functions like a PSTN area code prefix. The device will use the mapped IP address or configuration if the dialed number starts with the specified prefix. Prefix matching requires adding a "T" after the prefix to distinguish it from exact matches. The maximum length supported is 30 digits.
Note: Use two different special characters. - x: Matches any single digit. - [ ]: Specifies a range of digits; can be a range, separated by commas, or a list of digits.	
Destination	Configure the destination address. If configured for point-to-point calling, simply enter the IP address of the other end.
Port	Configure the signaling port for the other party's protocol. This is an optional setting, with the default being 5060.
Prefix	Configure an alias as an optional setting: it is used as a replacement number when the other party's number has a

	prefix.
Note: Aliases come in four types and must be set with the replacement length: 1）**Add**: Prefix xxx to the number, which helps users reduce dialing length. 2）**All**: Replace the entire number with xxx, enabling quick dialing. 3）**Delete**: Remove the first n digits of the number, where n is set by the replacement length. 4）**Replace**: Replace the first n digits of the number with xxx, where n is set by the replacement length.	
Suffix	Configure a suffix as an optional setting: this suffix will be appended to the end of the dialed number.
Length	Configure the replacement/deletion length to replace or delete digits from the user-entered number according to this length. This is an optional setting. For example, if the deletion length is set to 3, the first three digits of the number will be removed.

Examples of Alias Application

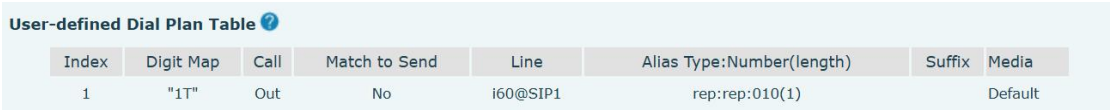
This feature allows users to create rules to simplify dialing. Several options are available for dialing rules. The following examples will demonstrate how it works.

Example 1: Replace All

If a user dials directly using IP point-to-point mode and the other party's IP is 172.168.2.208, you can configure a rule like the one shown below. With this rule, dialing 123 will call the user with IP address 172.168.2.208.

Example 2: Partial Replacement

For example, to dial a PSTN number in Beijing, you can set up the following dialing rule: all numbers starting with '1' will be processed by this rule. To call `010-62213123`, you would simply dial '162213123'.



Example 3: Add

Provide two examples.

Scenario 1: Assume that when a user dials any 11-digit number starting with 131, the system will automatically prepend a '0' before sending the call.

Scenario 2: Assume that when a user dials any 11-digit number starting with 135 to 139, the system will prepend a '0' before sending the call after receiving the full 11 digits.

Using two different special characters:

'x' represents any single digit;

'【】' specifies a range of digits, which can either be a range, separated by commas, or a list of specific digits.

With these rules, users can easily set up their own dialing rules and create dialing rules that are compatible with their server, greatly enhancing the convenience and practicality of the device.

5.4.4 Action Plan

Custom linkage rules can be added to achieve the desired linkage effect. For example, when the device calls a video phone, the linked IP camera will simultaneously transmit the video to the other device (if it supports video), and so on.

Parameters	Description
Number	Auxiliary device number (supports video)
Type	Supports displaying video during a call
Direction	Display video based on call type, incoming/outgoing
Line	Set the outgoing line
Username	Bind the phone's username
Password	Bind the phone's password
URL	Video stream information
UserAgent	Set user agent information
MCAST Codec	Set multicast codec
Action	Select linkage action

5.4.5 Basic Settings

STUN (Session Traversal Utilities for NAT) is a network protocol used to establish peer-to-peer communication in VoIP and video communication. It helps two devices connect through NAT or firewalls, allowing users to connect to other users or endpoint devices via the Internet. In simple terms, STUN helps users overcome network barriers and establish smooth, uninterrupted communication.

Parameters	Description
STUN Settings	
Server Address	Set the STUN server address.
Server Port	Set the STUN server port, default is 3478.
Binding Period	Set the STUN binding interval to ensure NAT traversal is enabled.
SIP Waiting Time	Set the timeout for STUN binding before transmitting SIP information.
SIP P2P Settings	
Enable Auto Answering	Enable automatic answering of IP call incoming after timeout.
Auto Answering Delay	Set the automatic answering timeout.
DTMF Type	Set the DTMF type for the line.
DTMF SIP INFO Mode	Set the SIP INFO mode to send '*' and '#' or '10' and '11'.

5.5 Intercom Settings

5.5.1 Features

Parameters	Description
Basic Settings	
Enable Call Waiting	Enabled by default. When enabled, it allows users to answer a second call while keeping the current call active.

Enable Auto On Hook	Configure whether to enable automatic hang-up and return to standby after the call ends.
Auto HangUp Delay	Configure the automatic hang-up time; if in hands-free mode, the device will automatically return to standby after exceeding the auto hang-up time.
Enable Silent Mode	When enabled, the device is in silent mode and will not ring on incoming calls; it can be unmuted using the volume and mute keys.
Disable Mute for Ring	When enabled, the mute key on the device will be ineffective.
Ban Outgoing	Disallow outbound calls; when enabled, lifting the handset will immediately provide a busy signal, prompting the user to hang up.
Default Ans Mode	Select the default call mode after an incoming call, including “video” and “audio.”
Default Dial Mode	Select the default call mode for dialing, including “video” and “audio.”
Enable Restricted Incoming List	Enable restriction for incoming call lists.
Enable Restricted Outgoing List	Enable restriction for outbound call lists.
Enable Country Code	Enable country code.
Country Code	Enter the country code.
Area Code	Enter the area code.
Allow IP Call	If enabled, the device allows direct IP calling; otherwise, it does not.
P2P IP Prefix	Set the prefix for point-to-point IP calls.
Restrict Active URI Source IP	Set the device to accept valid URI commands from specific IP addresses. Note: This feature is typically used for device management.
Push XML Server	Configure the XML server; when the phone receives a request, it will determine whether to display the content specified by the

	server for a given phone.
Line Display Format	Customize line format, such as SIPn/SIPn: xxx/xxx@SIPn.
Call Number Filter	Configure a special character '&'; if the other party's number is 78&9, the '&' will be filtered out during the call.
Auto Resume Current	Automatically release HOLD if the current route changes.
Limit Talking Duration	Automatically hang up the call after the configured time when enabled.
Talking Duration	Call duration settings: 20-600 seconds.
Call Timeout	Automatically hang up the call after the timeout if the call recipient does not answer.
启用推送 xml 身份验证	启用后推送 xml 消息，需要带用户密码密码
Ring Timeout	Automatically hang up the call after the timeout if the called party does not answer.
Description	Display description information in IP scanning tool software. Default is 'IP Video Doorphone' .
Tone Settings	
Enable Holding Tone	Enable to play a prompt tone during call hold.
Enable Call Waiting Tone	If this feature is disabled, no 'beep' prompt will be heard during call waiting.
Play Dialing DTMF Tone	DTMF prompt tones when pressing numeric keys during dialing: The device is enabled by default.
Play Talking DTMF Tone	DTMF prompt tones when pressing numeric keys during a call: The device is enabled by default.
Auto Answer Tone	When enabled, a 'beep' prompt tone will be heard during automatic answering.
Open Success Prompting	**Disabled:** No prompt tone after a successful door opening. **Default:** Uses the default prompt tone. **Voice:** Default built-in voice prompt, default is "Door open successful." Supports custom door open successful prompt tone. After upgrading the ringtone file in System - Upgrade - Ringtones, you

	can set a custom tone for successful door opening.
Open Failed Prompting	**Disabled:** No prompt tone after a door open failure. **Default**: Uses the default prompt tone. **Voice:** Default built-in voice prompt, default is "Door open failed." Supports custom door open failure prompt tone. After upgrading the ringtone file in System - Upgrade - Ringtones, you can set a custom tone for door open failure.
Close Door Prompting	**Disabled:** No prompt tone after door closing. **Default:** Uses the default prompt tone. **Voice:** Default built-in voice prompt, default is "Door closing." Supports custom door closing prompt tone. After upgrading the ringtone file in System - Upgrade - Ringtones, you can set a custom tone for door closing.
Issuing Success Prompting	**Disabled:** No prompt tone after successful card addition. **Default:** Uses the default prompt tone. **Voice:** Default built-in voice prompt, default is "Card added successfully." Supports custom card addition successful prompt tone. After upgrading the ringtone file in System - Upgrade - Ringtones, you can set a custom tone for successful card addition.
Issuing Failed Prompting	**Disabled:** No prompt tone after card addition failure. **Default:** Uses the default prompt tone. **Voice:** Default built-in voice prompt, default is "Card addition failed." Supports custom card addition failure prompt tone. After upgrading the ringtone file in System - Upgrade - Ringtones, you can set a custom tone for card addition failure.
Revoke Prompting	**Disabled:** No prompt tone after successful card deletion. **Default:** Uses the default prompt tone. **Voice:** Default built-in voice prompt, default is "Card deleted successfully."

	Supports custom card deletion successful prompt tone. After upgrading the ringtone file in System - Upgrade - Ringtones, you can set a custom tone for successful card deletion.
Revoke Failed Prompting	**Disabled:** No prompt tone after card deletion failure. **Default:** Uses the default prompt tone. **Voice:** Default built-in voice prompt, default is "Card deletion failed." Supports custom card deletion failure prompt tone. After upgrading the ringtone file in System - Upgrade - Ringtones, you can set a custom tone for card deletion failure.
Door Sensor Prompting	**Disabled:** No prompt tone for door magnetic detection abnormalities. **Default:** Uses the default prompt tone. **Voice:** Default built-in voice prompt, default is "Please close the door." Supports custom door magnetic detection prompt tone. After upgrading the ringtone file in System - Upgrade - Ringtones, you can set a custom tone for door magnetic detection abnormalities.
Intercom Settings	
Enable Intercom	When the intercom system is enabled, the device will automatically answer incoming call requests with the SIP header Alert-Info command.
Enable Intercom Mute	Enable mute function during intercom mode calls.
Enable Intercom Tone	A prompt tone will be heard for incoming calls in intercom mode.
Enable Intercom Barge	Automatically answer intercom mode calls during an ongoing call; if the current call is in intercom mode, new intercom mode calls will be rejected.
Response Code Settings	
Busy Response Code	Set the SIP response code for when the device is busy.
Reject Response Code	Set the SIP response code for call rejections.

5.5.2 Media Settings

Parameters	Description
Codecs Settings	Choose to enable or disable the following audio codecs: G.711A/U,G.722,G.729,ILBC,opus，G.726,G.723.1
Media Settings	
Default Ring Type	Configure preset ringtones. If no special ringtone is set for the incoming number, the default ringtone will be used.
免提音量设置	设置免提音量，音量为 1~9
免提铃声音量设置	设置免提铃声音量，音量为 0~9
Speakerphone SignalTone Volume	Set the volume for the hands-free signal tone, with a range of 0-9.
DTMF Payload Type	Enter the DTMF payload type, with a value between 96-127.
Handfree Mic Gain	Set the hands-free MIC gain, with a range of 1-9.
Opus Payload Type	Set the Opus payload type, with a range of 96-127.
OPUS Sample Rate	Set the Opus sampling rate to either OPUS-NB (8kHz) or OPUS-WB (16kHz).
ILBC Payload Type	Set the iLBC payload type, with a range of 96-127.
ILBC Payload Length	Select the iLBC payload length.
Enable VAD	Enable or disable voice activity detection.
Disable AEC	Enable or disable echo cancellation.
H.264 Payload Type	Set the H.264 Payload type, with a range between 96-127, default is 117.
Video Direction	Sendonly: Establish a video call where the SDP in the invite package is sendonly; Sendrecv: Establish a call where the SDP in the invite package is sendrecv.

RTP Control Protocol（RTCP）Settings	
CNAME user	Set the CNAME user.
CNAME host	Set the CNAME host.
RTP Settings	
RTP Keep Alive	While holding a call, send a packet every 30 seconds when enabled.
Alert Info Ring Settings（alert-info）	
Value	Set the value for the specified ringtone type for incoming calls.
Ring Type	Configure the built-in ringtone type settings.

5.5.3 Camera Settings

Parameters	Description
Connection Mode Setting	
Native Camera	**Local Camera:** Automatically use the local camera to transmit images. **IP Camera:** After setting up the external camera, automatically use the external camera to transmit images.
Camera Settings	
White Balance Mode	**Auto Mode**: The camera automatically adjusts based on the color temperature of the scene to compensate for the light source color. **Lock Mode**: Fixes the white balance parameters and does not adjust based on the actual color temperature. **Incandescent Lamp Mode:** Compensates for the color tone of incandescent light sources (e.g., bulbs, tungsten lamps, candles). Suitable for light sources with a yellowish hue. **Warm Light Mode:** Compensates for the color tone of warm light sources, suitable for light sources with a color temperature around 2700K.

	Natural Light Mode: Provides accurate color reproduction under natural sunlight, suitable for outdoor shooting with a wide range of uses. **Fluorescent Lamp Mode**: Compensates for the color tone of fluorescent light sources (e.g., daylight lamps, energy-saving lamps)
Exposure Mode	**Auto Mode**: The camera automatically sets the exposure parameters without manual adjustment. **Manual Exposure Time**: Set the exposure time manually, with a range of 0-10000. **Manual Exposure Gain**: Set the exposure gain manually, with a range of 0-1024. **All Manual**: Manually set the exposure time and gain.
Exposure Time	It's referring to the duration of pressing the shutter. Increasing the exposure time can improve the signal-to-noise ratio and make the image clearer. A longer exposure time allows more photons to accumulate on the CCD/CMOS surface, resulting in a brighter image. However, if the exposure is too long, the image may become overexposed and lose detail; if the exposure is too short, the image may be too dark.
Exposure Gain	It refers to the amplification gain of the analog signal after double sampling. However, when amplifying the image signal, noise signals are also amplified. Gain is typically used when the signal is weak but you do not want to increase the exposure time.
Contrast Mode	**Auto Mode**: The camera automatically adjusts the contrast based on the environment, requiring no manual adjustments from the operator. **Manual Mode**: Manually set the camera's contrast parameters.
Contrast	Contrast refers to the degree of difference between the light and dark areas of an image. Increasing the contrast makes the bright areas brighter and the dark areas darker, enhancing the overall difference

	between light and dark.
Saturation Mode	**Auto Mode**: The camera automatically adjusts the saturation based on the environment, requiring no manual input from the operator. **Manual Mode:** The saturation level is manually set by the operator.
Saturation	Saturation adjusts color intensity. Higher values exaggerate colors, while lower values reduce them. At the lowest setting, the image becomes black and white.
Sharpness Mode	**Auto Mode**: The camera automatically adjusts sharpness based on the environment, no manual adjustment needed. **Manual Mode:** Manually adjust the camera's sharpness settings.
Sharpness	Sharpness, sometimes called "clarity," indicates the level of detail and edge definition in an image. Increasing sharpness enhances contrast and makes details appear clearer.
Wide Dynamic	Enable or disable Wide Dynamic Range (WDR). Enabling WDR allows the camera to capture images in high-contrast environments.
WDR	Adjust image brightness manually, with a range of 0 to 10.
Enable IRCUT	Enable or disable IRCUT.
Image Mode	**Day (Color):** The camera transmits color images in bright daylight. **Night (Black & White):** The camera transmits black and white images in low light conditions at night. **Auto:** The camera automatically switches between color images in bright daylight and black and white images in low light conditions.
Brightness	Set the image brightness manually, with a range from 0 to 100.
Enable Onvif	Enable or disable the ONVIF protocol. When enabled, devices can be discovered by ONVIF-supported recorders.
Call Stream	Choose between the main stream or sub-stream for video calls.
Enable Onvif Auth	Specify if authentication (username and password) is required when using ONVIF protocol.
Enable Rtsp Auth	Specify if authentication (username and password) is required when using RTSP protocol.
H.264 Payload	Set the payload type for H.264, within the range of 96 to 127.

Type	
Osd Settings	
OSD Time	Enable/disable the date display on the camera image interface.
OSD Text	Enable/disable the text display on the camera image interface.
Video Codecs	
编码格式	支持H.264编码格式
Bitrate Control	VBR: Adapts the bit rate during video calls for better video quality. CBR: Maintains a fixed bit rate based on the set value during video calls.
Resolution	Supports 1080P，720P，4CIF,VGA,CIF,QVGA
Frame Rate (fps)	The higher the value, the smoother the video, but it requires higher network bandwidth; not recommended to adjust.
BitRate	It refers to the data usage of a video file per unit time, also known as bitrate or stream rate. In simpler terms, it's the sampling rate and is a crucial part of video encoding for controlling image quality. Common units used are kb/s or Mb/s.
I Frame Interval	The higher the value, the worse the video quality; otherwise, the video quality is better. Adjusting this is not recommended.
RTSP Information	
H264 Main Stream Url	Copy and paste the main stream URL into the VLC player, or click [Preview] to display the current camera video.
H264 Sub Stream Url	Copy and paste the sub-stream URL into the VLC player, or click [Preview] to display the current camera video.
SnapShot	
Snapshot By Input	Select the input port to trigger snapshot capture.
Snapshot By State	Select the call status to trigger snapshot capture.
Snapshot By Motion Detection	Enable motion detection snapshot capture. When motion is detected near the camera, a snapshot will be taken.

Snapshot Save	Set the method for saving snapshot images, including: "Server," "Storage Card," or "Server and Storage Card." The SD card supports up to 128GB. When selecting SD card, ensure that the SD card is inserted.
Server Url	Enter the server address.
Username	Enter the username.
Password	Enter the password.

5.5.4 MCAST

The multicast feature allows users to easily send announcements to all multicast members. By configuring the multicast key on the device, it sends a multicast RTP stream to a predefined multicast address. The device can also be configured to listen to a multicast address, receiving and playing the RTP stream sent to that address.

Parameters	Description
Sip Priority	Define the priority level for an ongoing call, with 1 being the highest priority and 10 being the lowest priority.
Enable Page Priority	Regardless of which multicast call comes in first, the device will prioritize answering the multicast with the higher priority.
Enable Prio Chan	Once enabled, connections can only be established on the same port and channel. Channel 24 is the priority channel, higher than channels 1-23; a channel value of 0 indicates that the channel is not used.
Enable Emer Chan	Once enabled, channel 25 has the highest priority.
Name	Server name for listening to multicast
Host:port	Server address for listening to multicast: Port number
Channel	0-25 (24 is the priority channel, 25 is the emergency channel)

MCAST Listening:

- On the webpage, go to [Function Key] >> [Function Key Settings], select the type as MCAST Paging, set the multicast address, and choose the encoding.

- After configuration, click Apply.
- On the receiving device's webpage, go to [Intercom Settings] >> [MCAST], set the multicast name, host, and port.
- Press the configured DSS key for multicast.
- The receiver will receive the multicast call and automatically play it.

MCAST Dynamic:

Function Description: Multicast configuration information is delivered via SIP Notify signaling. After receiving the information, the device configures it in the system for multicast listening or cancels multicast listening in the system.

5.5.5 Action

It is mainly for Action URL settings, configuring the URL to report actions to the server.

5.5.6 Time/Date

Users can configure the device's time settings on this page.

Parameters	Description
Network Time Server Settings	
Time Synchronized via SNTP	Enable time synchronization using the SNTP protocol.
Time Synchronized via DHCP	Enable time synchronization using the DHCP protocol.
Time Synchronized via DHCPv6	Enable time synchronization using the DHCPv6 protocol.
Primary Time Server	Set the primary time server address.
Secondary Time Server	Set the backup time server address. When the primary server is unavailable, the device will attempt to connect to the backup time server for time synchronization.
Time zone	Select the time zone.
Resync Period	Resynchronize with the time server.

12-hour clock	Set the 12-hour time display mode.
Time/Date Format	Select the date/time display format.
Daylight Saving Time Settings	
Location	Select your location.
DST Set Type	Set the DST (Daylight Saving Time) type
Fixed Type	The DST rule is based on either a specific date or a relative rule for date calculation. In automatic mode, this is read-only.
Offset	Adjust the time forward/backward when DST starts/ends.
Month Start	DST start month
Week Start	DST start week
Weekday Start	DST start weekday
Hour(s) Start	DST start hour
Month End	DST end month
Week End	DST end week
Weekday End	DST end weekday
Hour(s) End	DST end hour
Manual Time Settings	Manually set the current time.

5.5.7 Time Plan

Users can set specific times or time periods for the device to perform certain actions.

Parameters	Description
Name	Enter a custom name.
Type	Scheduled reboot, scheduled upgrade, scheduled sound detection, scheduled audio playback, scheduled door unlocking.
音频路径	支持本地 本地：选择本地上传的音频文件
音频设置	选中要播放的音频文件，支持试听，点击试听后可以立即播放
Repetition period	No repetition: Execute the action once within the specified time

	range. Daily: Execute this action every day within the same time range. Weekly: Execute this action on specific weekdays within the specified time range. Monthly: Execute this action on specific dates within the specified time range.
Effective Time	Set the time period for execution

5.5.8 Tone

Users can configure the device's alert tones on this page. They can either select a country/region or define a custom region. Selecting a region will automatically populate the relevant information below, while choosing a custom region allows modification of key tones, ringtone, and other settings.

5.5.9 Led

Users can configure the device's indicator light status and color on this page.

status light: Users can customize the LED indicators and colors for various device states.

Save Power: When the device is not in use, it automatically turns off the indicator lights. Users can enable or disable power saving mode.

Timeout To Power Saving: The device enters power saving mode after a set period of inactivity. The default is 60 seconds.

After entering power saving mode, if the device detects nearby movement, it automatically exits power saving mode and illuminates the indicator lights according to the device's status.

5.6 Call List

5.6.1 Call List

Restricted Incoming Calls:

It functions similarly to a blacklist. By adding a number to the blacklist, users will no longer receive calls from that number until they remove it from the list. Users can add specific numbers to the blacklist or add specific prefixes to block calls from all numbers with those prefixes.

Restricted Outgoing Calls:

Add restricted outbound numbers; once added, calls to those numbers will be blocked until the number is removed from the list.

5.6.2 Web Dial

You can use the webpage to make, answer, and end calls.

5.7 Function Key

Parameters	Description
Function Key Settings	
Memory Key	**Speed Dial**: Users can directly dial pre-set numbers. This feature is convenient for calling frequently used numbers. **Intercom**: This feature allows operators or secretaries to quickly connect calls, and is widely used in office environments.
Key Event	Users can choose a function key as a shortcut for triggering events Handfree: One-touch activation of speakerphone Audio play: Play music locally OK: Confirmation button Volume Up: Increase volume Volume Down: Decrease volume Redial: Redial the last number called Release: Release the call Call Back: Call back the last incoming call Volume Circle: Cycle through volume adjustments
DTMF	During a call, pressing this button sends the configured DTMF tones.
MCAST Paging	Configure the multicast address and audio encoding. Pressing this key initiates the multicast.
Action URL	Users can use specific URLs to perform basic operations on the

	device, such as making calls or opening doors.
MCAST Listening	In standby mode, pressing the function key will make the device listen to the multicast if the RTP of that multicast is detected.
PTT	**Speed Dial**: Press to initiate a call and talk; release to end the call. **Intercom**: Press to start intercom communication; release to end the intercom session. **Multicast**: Press to start multicast; release to end the multicast.
Programmable Key Settings	
Desktop	Invalid: Pressing the speed dial key has no response. Dsskey1: When set to dsskey1, it follows the settings of dsskey1 to make calls, answer calls, etc.
Dialer	Invalid: Pressing the speed dial key has no response. Dsskey1: When set to dsskey1, it follows the settings of dsskey1 to make calls, answer calls, etc.
Ringing	Answer: Set to answer calls. When an incoming call arrives, if auto-answer is not enabled, pressing the speed dial key will answer the call. End: Set to end calls. When there is an incoming call, pressing the speed dial key will hang up the call.
Talking	End: Set to end calls. When on a call, pressing the speed dial key will hang up the call. Volume Up: Set as the volume increase key. During a call, pressing the speed dial key will increase the volume. Volume Down: Set as the volume decrease key. During a call, pressing the speed dial key will decrease the volume. Dsskey1: Set as dsskey1. During a call, pressing the speed dial key will perform actions according to the settings of dsskey1, such as making or answering calls.
Advanced Settings	

Dial Mode Select	Number 1 to Number 2 Call Transfer Mode Selection. <Main-Secondary>: If the first number is not answered within the set time, the call automatically switches to the second number. <Time Period>: The system automatically detects the current time during a call. If it is within the time period for Number 1, it will call the first number; otherwise, it will call the second number.
Call Switched Time	Set the time for transferring from Number 1 to Number 2, default is 16 seconds.
First Number Start Time	When defining the time period mode, set the start time for Number 1. Default is '06:00'.
First Number End Time	When defining the time period mode, set the end time for Number 1. Default is '18:00'.

5.8 Security

5.8.1 Web Filter

Users can configure the device to allow access only from machines within a specific IP subnet.

Add and delete allowed IP subnets. Configure the starting IP address in the 'Start IP' field and the ending IP address in the 'End IP' field, then click [Add] to successfully add it. You can set a large subnet or divide it into several subnets for addition. To delete a subnet, select the starting IP address of the subnet to be deleted from the list, then click [Delete] for the changes to take effect.

5.8.2 Trust Certificates

On this page, you can upload and delete previously uploaded certificates.

5.8.3 Device Certificates

Select the device certificate as the default certificate or a custom certificate. You can

upload and delete the uploaded certificates.

5.8.4 Firewall

This page allows you to enable or disable the input and output firewalls, as well as configure the firewall's input and output rules. These settings can help prevent malicious network access or restrict internal users from accessing certain external network resources, thereby enhancing security.

The firewall rule setup is a simple firewall module. This feature supports two types of rules: input rules and output rules. Each rule is assigned a sequence number, with a maximum of 10 rules allowed for each type.

Considering the complexity of firewall settings, the following will illustrate an example:

Parameters	Description
Enable Input Rules	Indicates enabling the input rule application.
Enable Output Rules	Indicates enabling the output rule application.
Input/Output	Select whether the currently added rule is an input or output rule.
Deny/Permit	Select whether the current rule configuration is to deny or allow.
Protocol	The protocol types for filtering include four options: TCP, UDP, ICMP, and IP.
过滤端口范围	过滤的端口范围
Src Address	For the source address. The source address can be a host address, a network address, or the wildcard address 0.0.0.0. It can also be a network address like *.*.*.0, such as 192.168.1.0.
Dst Address	For the destination address. The destination address can be a specific IP address, or the wildcard address 0.0.0.0. It can also be a network address like *.*.*.0, such as 192.168.1.0.
Src Mask	For the source address mask. When set to 255.255.255.255, it indicates a specific host. When set to a subnet mask like 255.255.255.0, it indicates that the filter applies to a network

	segment.
Dst Mask	For the source address mask. When set to 255.255.255.255, it indicates a specific host. When set to a subnet mask like 255.255.255.0, it indicates that the filter applies to a network segment.

5.9 Device Log

On this page, you can capture device logs. In case of any issues, the logs can be sent to technical support for troubleshooting.

5.10 Security Settings

On this page, you can configure security input and output settings.

Parameters	Description
Basic Settings	
Ringtone Duration	Alarm ringtone duration.
Input & Tamper Server Address	Configure the remote response server address (including the remote response server address and the alarm trigger server address). When the input port is triggered, a short message will be sent to the server with the following format: Alarm_Info:Description=i16SV;SIP User=;Mac=0c:38:3e:39:6a:b6;IP=172.16.7.189;port=Input
Message	Fill in the information attached when uploading to the server.
Input Settings	
Input	Enable or disable the input port.
Triggered By	When selecting low-level trigger (closed trigger), the system detects a closed trigger on the input port (low level).
	When selecting high-level trigger (open trigger), the system detects an open trigger on the input port (high level).
Input Duration	

Triggered Action: Send SMS	Enable or disable the input port's ability to send messages to the server.
Event	Select the time after the input port is triggered, including options for door sensors, switches, and Dsskey.
Triggered Ringtone	Supports ringtone selection.
Output Settings	
Enable Logs	Enable or disable the log.
Triggered By URI Ringtone	Supports ringtone selection.
Triggered By SMS Ringtone	Supports ringtone selection.
Triggered By Dsskey Ringtone	Supports ringtone selection.
Output	Enable or disable the output port.
Standard Status	When selecting low level (NO: open), the NO port will open when the trigger condition is met.
	When selecting high level (NC: closed), the NC port will close when the trigger condition is met.
Output Duration	Output port change duration, with a default value of 5 seconds.
Output Trigger Mode	When the input port meets the trigger condition, the output port will be triggered (the port level change duration is controlled by the <Output Duration> setting).
Trigger By Active URI	Enable or disable URI triggering. When a command is sent from a remote device or server, if it is correct, the corresponding output port will be triggered or reset.
Trigger Message	Message sent after triggering the output port.

Reset Message	Message sent after resetting the output port.
Trigger By SMS	Enable or disable SMS triggering. When a command `ALERT = [command]` is sent from a remote device or server, if it is correct, the corresponding output port will be triggered or reset.
Trigger Message	Message sent after triggering the output port.
Reset Message	Message sent after resetting the output port.
Trigger By Input	Select the required input port to trigger the current input port.
Trigger By Call State	Port output continuous time trigger types, including trigger conditions. For example: When a call triggers the output port, the output port will remain active for the duration of the call. 1. Talking 2. Ringing 3. Calling
Trigger By DssKey	DSS trigger output.
Dsskey Trigger Condition	Trigger the output port after hanging up.
Hangup Delay	Hang-up trigger delay time, with a default of 5 seconds.
Motion Detection Settings	
Motion Detection Alarm	Distance can be set to 0 or between 10 and 180 cm. Setting it to 0 means the feature is turned off.
Trigger Duration	Set the trigger delay time, with a default of 3 seconds and a range of 0 to 3600 seconds.
Triggered Ringtone	Supports ringtone selection.

Triggered Action: Send SMS	Enable or disable the input port's ability to send messages to the server.
Key Event	Set to `dsskey1` for making calls, default is `none`.
Tamper Alarm Settings	
Enable Tamper Alarm	Enable or disable tamper detection. If the terminal is forcibly removed, tamper detection will be triggered, and the configured alarm ringtone will play continuously.
Alarm Command	Trigger an alarm and simultaneously send the `Alarm command` set to the next server.
Reset Command	To stop the alarm ringtone, the remote side can send a short message to the terminal. The content of the short message should be the value set in the `reset command`. The terminal will then stop playing the alarm ringtone.
Alarm Ringtone	Alarm ringtone settings.
Tamper Alarm Reset	
Reset Alarm Status	Reset to stop the ringtone playback.

5.11 EGS Setting

5.11.1 Feature

You can configure the basic settings for access control through this interface.

Table 34 - Access Control Function Settings Parameters

Parameters	Description
Basic Settings	
Relay1 Mode	单稳态：门禁只有开门一种模式 双稳态：门禁有开门与关门两种模式，再次触发后会变为另一种模式，并一直保持。

Relay1 Open Duration	单稳态模式有效，门禁开门时间，超时后自动关闭。默认 5 秒
Wiegand Format	支持的韦根门禁卡的格式
Wiegand Mode	韦根模式可选 in 和 out 两种模式，默认为 in
Wiegand Type	支持韦根 26 和 34 两种
Card Reader Working Mode	Normal：刷卡后可以打开门禁； Card Issuing：这个状态下刷卡可以把卡添加到数据库； Card Revoking：这个状态下刷卡可以把卡从数据库中删除。
Relay Open Mode	继电器打开方式可选读卡器、密码、蓝牙。配合APP使用蓝牙开门时，在此处必须打开蓝牙
Keypad Input Mode	This feature is only available on the i60K model. Disable: Disables keypad input. Password Only: Only the password can be used to unlock the door. Dial Only: The keypad can only be used for dialing and calling. Dial & Password: If the password is "1234", press the keypad and enter 1234 # to unlock the door. To dial an IP address, enter *172*18*28*14 #. Password & Dial: If the password is "1234", press the keypad and enter *1234 # to unlock the door. To dial an IP address, enter 172*18*28*14 #.
开门日志上报	可在此处上报开门日志上报的服务器地址、日志格式等

5.11.2 Relay

Parameters	Description
Description	
Door Sensor1	Enable or disable Door Sensor 1.
Door Sensor Check Delay1	Door Sensor 1 detection delay time setting, with a default of 5 seconds.
Relay Status1	Open/Close
Door Sensor Status	Open/Close
Relay Control	

Relay	Execute a door lock operation to open or close the door.
Action	Perform the open/close action.
Mode	Once: Executes the open action; the door will automatically close after a timeout. Always: Executes the open action without automatic closure; manual closure is required.

5.11.3 Personnel Management

The device supports adding users and granting access via card, password, or facial recognition. Once access is granted, users can unlock the door using their card, password, or facial recognition at the device.

User parameters:

Parameters	Description
Name	User's Name
Card Number Type	**Normal**: A standard door access card. **Add**: When the device is in standby, swipe the "Add Card Administrator Card" to enter add card mode. After that, swipe the card to add unregistered cards to the list. Once the process is complete, swipe the "Add Card Administrator Card" again to switch the device's reader back to standard mode. **Del**: When the device is in standby, swipe the "Delete Card Administrator Card" to enter delete card mode. After that, swipe the card to remove registered cards from the list. Once the process is complete, swipe the "Delete Card Administrator Card" again to switch the device's reader back to standard mode.
Card Number	Access card ID number (the first ten digits of the access card number, e.g., 0004111806).

	If configuring the access card number on the web interface, you will need to swipe the card on the device once. Then, check the card number in the access log page and copy it here.
Password Type	**Local:** This is the local door access password. When in standby mode, enter the set password on the keypad to immediately unlock the door. **DTMF:** 远程 DTMF 密码，用于在通话过程中，在远端室内机、App 上输入此密码进行远程开门。注：此功能适用于 i60K **本地和 DTMF：**选择此类型时，此密码可同时用于本地密码开门和远程 DTMF 开门。注：此功能适用于 i60K
Password	Door access password
Number	When the indoor unit calls the access control system or the access control system calls the indoor unit to open the door, a DTMF password is entered to unlock the door. Upon receiving the password, the device will compare the number and DTMF password. The door will only unlock if both the number and the corresponding DTMF password match successfully.
Location	After setting, this number can be used to replace the main number for calling.
CallForward	When the main number cannot be reached, the call will forward to this number.
Relay	Choose the door lock to be opened.
Times	This sets how many times the door can be unlocked within a specific time period. If the default configuration leaves this field blank, there is no limit on the number of uses. If a limit is set, the access will be "disabled" once the usage count is reached.
Source	Indicates whether the user data originates from the local device or the server. Manual: Manually added. Server: Delivered through the server.

Note:

Using the "Add Card Administrator Card" and "Delete Card Administrator Card" requires great caution. If you forget to switch the reader mode back to standard mode, it could damage user data and compromise access security.

5.11.4 Time Profile

Parameters	Description
Import Profile List	
Click **[Select]** to choose the time list file `timeProfileList.csv`, then click **[Update]** to batch import the time periods.	
Period Add	
Name	Set the time period name
Repetition Period	No repetition: The door is valid only during the specified time period; invalid at other times. Daily: The door is valid during the specified time period every day; invalid at other times. Weekly: The door is valid during the specified time period each week; invalid at other times. Monthly: The door is valid during the specified time period each month; invalid at other times.
Effective Time	Set activation time

5.11.5 Logs

Parameters	Description

Relay	Door lock
Result	Displays the result of a single door opening attempt success or failure
Name	Name of the person who opened the door
Source	Displays the card number or password used to open the door
Type	Opening method including password, card swipe, etc.
Reason	Reason for door opening failure
Time	Opening time

6 Troubleshooting

When the device is not functioning properly, users can try the following methods to restore normal operation or collect relevant information to send a problem report to the technical support email.

6.1 Obtain Device System Information

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

1. System Information（Model, MAC address, software and hardware versions）etc.
2. Network
3. SIP Accounts

6.2 Reboot

Restart the device through the web interface:

Click [System] >> [Reboot], and then press [Reboot].

Power cycle the device:

Simply unplug the power and then restart the device.

6.3 Reset Phone

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

Restore the device through the device interface:

Click [System] >> [Reset Phone] on the device, and then press [Reset].

6.4 Network Data Capture

Network data packets can be helpful in diagnosing device issues. To obtain the device's data packets, users need to log in to the device's web page, open [System] >> [Tools], and then click [Start] in [Web Capture] to begin capturing. A prompt will appear asking the user to save the captured file. Users can then perform related operations, such as starting/stopping the line or making calls. Afterward, click [Stop] on the web page. The

network data packets during this period will be saved in the file. Users can analyze the packets or send them to the technical support email.

6.5 Obtain Log Information

When encountering issues, log information can be helpful. To obtain the device's log information, users can log in to the device's web page, go to [Syslog], click the [Apply] button, and follow the steps until the issue occurs. Afterward, click the [Stop] button and [Export Log] to save it locally for analysis or send the log to technical support for troubleshooting.

6.6 Common Fault Cases

Fault Cases	Solution
Device will not start	1. The device is powered by a power adapter. Please use a compliant power adapter and ensure the device is properly connected to the power source. 2. The device is powered via POE. Please use a compliant POE switch.
设备无法注册到服务供应商	1. Please check if the device is connected to the network. 2. Check if the device has an IP address. If the IP address is 0.0.0.0, it means the device has not obtained an IP address. Verify that the network configuration is correct. 3. If the network connection is good, check your line configuration again. If all configurations are correct, contact your service provider for support or follow the instructions in “Network Data Capture” to obtain the network data packets and send them to the support email for further analysis.