MIU Magnet Gateway User Manual

Version 2.0

Address: Room 624, 6/F, Tsinghua Information Port, Shukan Building, Qingxiang Road, Longhua Street, Longhua District, Shenzhen 518109
Tel: +86-755-66630978, 82535461, 82535362
Sales: sales@openvoxtech.com
Technical Support: support@openvoxtech.com
Business Hours: Monday to Friday, 09:00-18:00 (GMT+8), excluding holidays

Thank you for choosing OpenVox products.

Revision History

Version	Release Date	Description
2.0	25/5/2026	Full update

1. Overview

1.1 Product Introduction

Magnet Gateway is a device with both Magnet trunk interfaces and network interfaces. It is used to implement voice communication between Magnet trunks and VoIP networks, and can also be understood as a Magnet-to-VoIP conversion device. In communication systems such as military or railway systems, traditional PBXs often provide only Magnet interfaces. These systems are relatively independent and are difficult to interconnect with existing telephone networks or next-generation networks (NGN). With the development of VoIP technology, retaining existing Magnet communication systems while connecting them to VoIP networks has become a common requirement. Magnet Gateway is designed for this type of integration scenario.

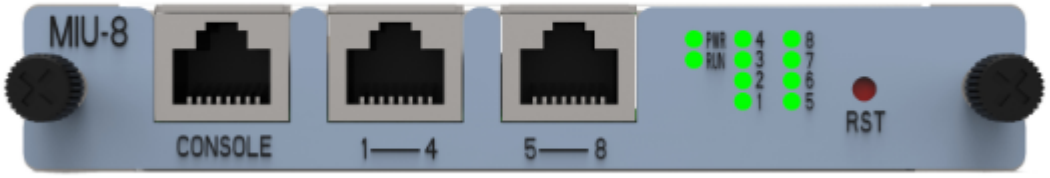
1.2 Product Models

MIU currently has two product models: MIU-4 and MIU-8. They provide 4 Magnet channels and 8 Magnet channels respectively.

1.3 Product Images

The MIU-4 panel is shown below.

The MIU-8 panel is shown below.



1.4 Physical Specifications

Item	Specification
Port protocol	Standard SIP, TCP/IP
Dimensions	160 x 100 mm
Weight	178 g

Item	Specification
Maximum power consumption	6.5 W
Storage temperature range	-40 deg C to 125 deg C
Operating temperature range	0 deg C to 50 deg C
Operating humidity range	10% to 90%

1.5 Software

- Default MIU IP: 172.16.80.X
- Username: admin
- Password: admin

During first login, you can access the device through the default IP address 172.16.80.x, where x indicates the slot number. For example, slot 1 indicates IP address 172.16.80.1. If the default username and password are used, the system prompts you to change the password at each login. After the password has been changed, this prompt is no longer displayed.

2. System

2.1 Status

After entering the system page, you can view port status, SIP messages, routing status, and basic network information directly. Detailed fields are shown in the figure below.

2.2 Time Settings

On this page, you can select the time zone and synchronize time automatically through NTP.

The fields for time settings are described in Table 2-1.

Option	Definition
System Time	System time of the gateway
Time Zone	World time zone. Select a city that is the same as or close to your city.
POSIX Time	POSIX time zone string
NTP Server 1	Primary time synchronization server or host name, for example: time.asia.apple.com
NTP Server 2	First backup NTP server, for example: time.windows.com
NTP Server 3	Second backup NTP server, for example: time.nist.gov
Save Data	Click this option to save modified time settings.
Synchronize Automatically from NTP Server	Whether to enable automatic time synchronization from an NTP server. On means enabled, and OFF means disabled.

2.3 Login Settings

On this page, users can perform the following operations:

- View and modify the Web login username and password, whether HTTPS-only login is required, and the HTTP port.
- View and modify SSH connection settings.
- Upload and update HTTPS certificates.

The options related to login settings are shown below.

Table 2-2 Web Login Settings

Option	Definition
System Time	System time of the gateway
Time Zone	World time zone. Select a city that is the same as or close to your city.
POSIX Time	POSIX time zone string
NTP Server 1	Primary time synchronization server or host name, for example: time.asia.apple.com
NTP Server 2	First backup NTP server, for example: time.windows.com
NTP Server 3	Second backup NTP server, for example: time.nist.gov
Save Data	Click this option to save modified time settings.
Synchronize Automatically from NTP Server	Whether to enable automatic time synchronization from an NTP server. On means enabled, and OFF means disabled.

Table 2-3 SSH Login Settings

Parameter Name	Description	Recommended Configuration
Enable	Set whether to enable SSH login.	Enable it when remote maintenance is required.
Username	Set the SSH login account.	A dedicated administrator account is recommended.
Password	Set the SSH login password.	A strong password is recommended.
Port	Set the SSH listening port.	A non-default port is recommended.

Table 2-4 HTTPS Certificate

Parameter Name	Description	Recommended Configuration
Certificate Upload	Select the HTTPS certificate file to upload.	Upload a valid certificate file.
Upload	Import the selected certificate into the device.	Execute after confirming the file is correct.
Save	Save the current configuration.	Save promptly after upload.

2.4 General Settings

This page is mainly used for basic system function configuration, including language switching, scheduled reboot, and other common options. It is recommended to apply unified settings according to project delivery requirements for later operation and maintenance.

Click System Information -> General to configure language settings and scheduled reboot.

2.5 Tools Page

This page is mainly used for system maintenance operations, including device reboot, firmware upgrade, configuration file backup and restore, and other functions. Before performing related operations, it is recommended to back up the current configuration.

Click System Information -> Tools to restart the device, upgrade firmware, upload configuration files, back up, restore, and restore the system.

2.6 System Information

This page is mainly used to view current system operation information, which is useful for installation, debugging, and troubleshooting. It is recommended to check related status items during delivery acceptance and routine inspection.

Product Name:	MIU
Serial Number:	02C001818FD427B9
Software Version:	1.1.55
Hardware Version:	1.0.0
Slot Number:	4
Storage Usage:	1.3M/54.1M (3%)
Memory Usage:	67.4993 % Memory Clean
Build Time:	2023-08-23 09:51:21
Contact Address	Room 624, 6/F, TsingHua Information Port, QingQing Road, LongHua Street, LongHua District, ShenZhen
Tel	+86-755-82535461
Fax	+86-755-83823074
E-Mail	support@openvox.cn
Web Site:	http://www.openvox.cn
System Time:	2023-8-27 14:04:36
System Uptime:	4 days 04:13:04

3. Analog Settings

Go to the `Analog Settings` menu. In Advanced Options, you can configure the following sections.

3.1 Entering the Channel Settings Page

This section describes how to enter the channel settings page. Users can enter the corresponding menu and click the edit icon to configure a single Magnet channel in detail.

Go to `Channel Settings` -> `Channel Settings`, and click the edit icon. 

Port	Type	Name	Line Status/Sip Account	Actions
1	MAG	mag-1	Connected	
2	MAG	mag-2	Connected	
3	MAG	mag-3	Connected	
4	MAG	mag-4	Connected	
5	MAG	mag-5	Connected	
6	MAG	mag-6	Connected	
7	MAG	mag-7	Connected	
8	MAG	mag-8	Connected	

3.1.1 Channel Configuration Details

After entering the channel settings page, configure parameters as needed.

Parameter descriptions are as follows:

Parameter Name	Description	Recommended Configuration
Name	Set the channel name.	Use an easily identifiable port name.
Dial by Key Press Count	Set the dialing trigger condition.	Configure according to service requirements.
Enable Wait for Answer	Set whether to enable waiting for answer.	Keep the default setting in most cases.
Auto Answer	Set auto-answer parameters.	Keep the default setting when auto-answer is not required.
Wait for Answer	Set the answer waiting time.	Set according to site requirements.
Silence Detection Threshold	Set the silence judgment threshold.	Keep the default setting in most cases.
Enable Wait for Hangup	Set whether to enable hangup waiting.	Enable it when false detection must be avoided.
Wait for Hangup	Set the hangup delay time.	Configure according to the actual scenario.

Parameter Name	Description	Recommended Configuration
Caller Number	Set the number displayed externally.	Enter the service number.
Caller ID Full Name	Set the caller ID display name.	Use the channel name.

3.2 Advanced Settings

This page is mainly used to configure advanced voice parameters for Magnet channels, including DTMF, echo processing, ringing duration, and intervals. If there are no special requirements, keep default values first, and then adjust them based on site test results.

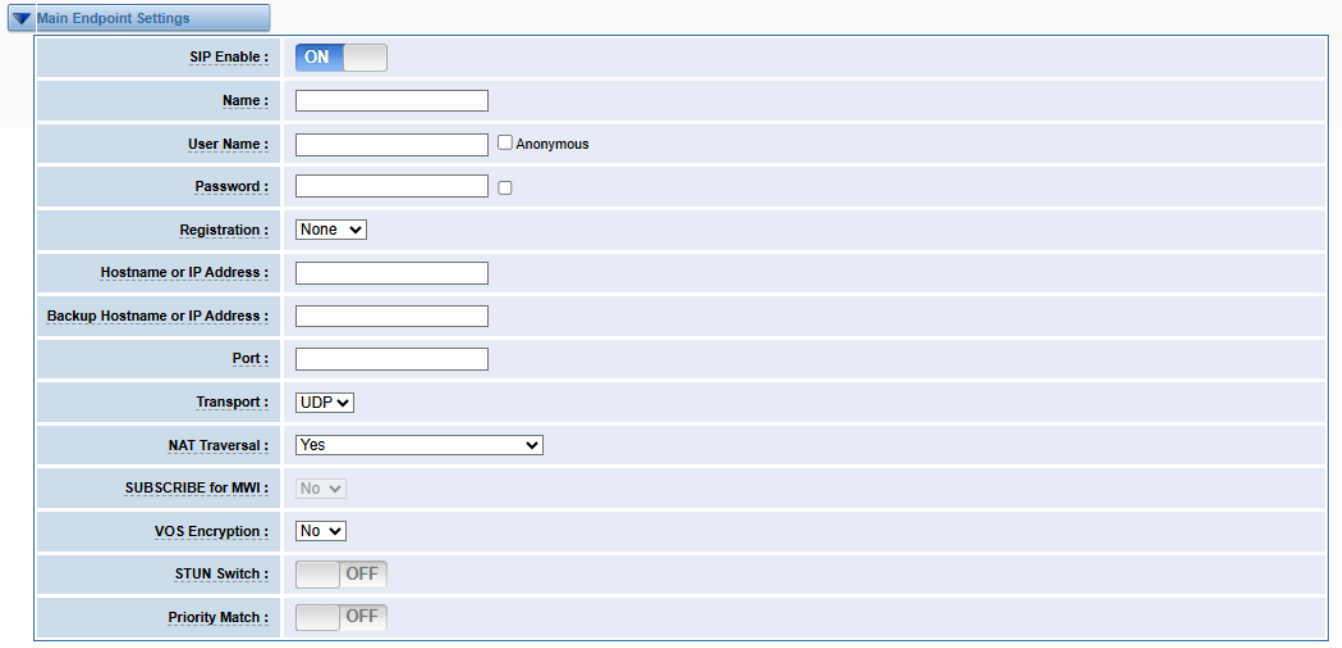
Parameter Name	Description	Recommended Configuration
Send DTMF During Call	Set whether to send key signals during a call.	Enable when IVR is required.
Echo Algorithm Type	Set whether to enable echo processing.	Enabling it is generally recommended.
Echo Cancellation Signal Length	Set the echo cancellation length.	Usually keep the default setting.
Ring Time	Set ring-related duration.	Configure according to the actual line.
Interval Time	Set the interval between actions.	Usually keep the default setting.

4. SIP Settings

Go to `SIP Settings` -> `SIP Endpoint`. The SIP settings page allows you to add and delete SIP endpoints, create SIP accounts in batches, configure advanced SIP settings, and configure SIP account security.

4.1 Add SIP Endpoint

4.1.1 Main Peer Settings

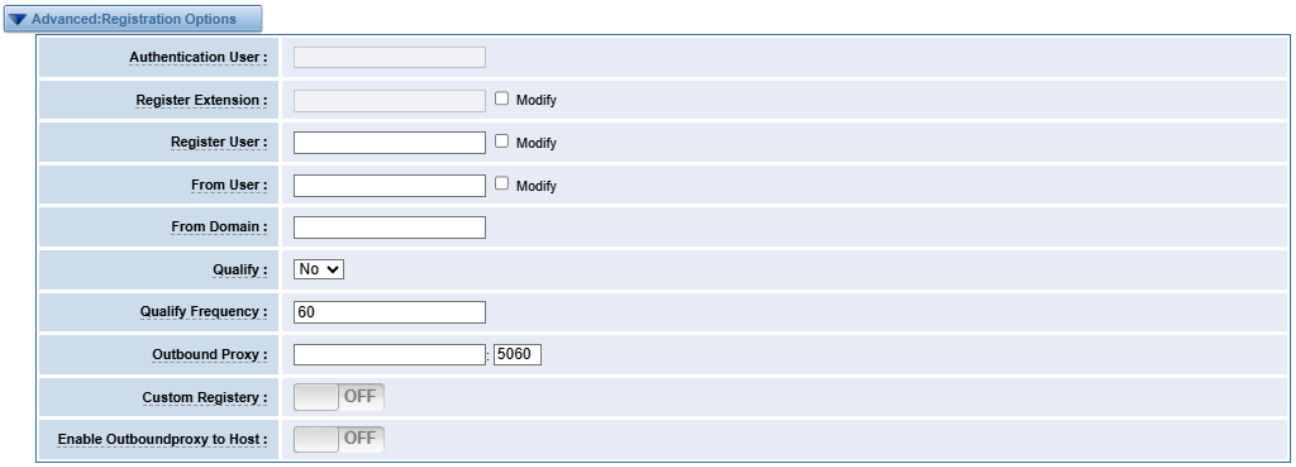


The meanings of specific fields are shown in the table below.

Field Name	Description	Configuration Recommendation
SIP Enable	Used to enable or disable the current SIP peer configuration. The SIP peer configuration takes effect only after this option is enabled.	After adding a configuration, set it to ON if it needs to be used immediately.
Name	Name of the current SIP peer, used for local identification and distinguishing different SIP peers.	Use an easy-to-identify name, such as "HQ IMS" or "Branch SIP Trunk".
Username	Username used for SIP registration or authentication.	Usually provided by the SIP server or carrier, and usually the same as the extension number, account, or authentication ID.
Anonymous	Controls whether the user identity is sent anonymously.	Keep it disabled by default if there are no special requirements.

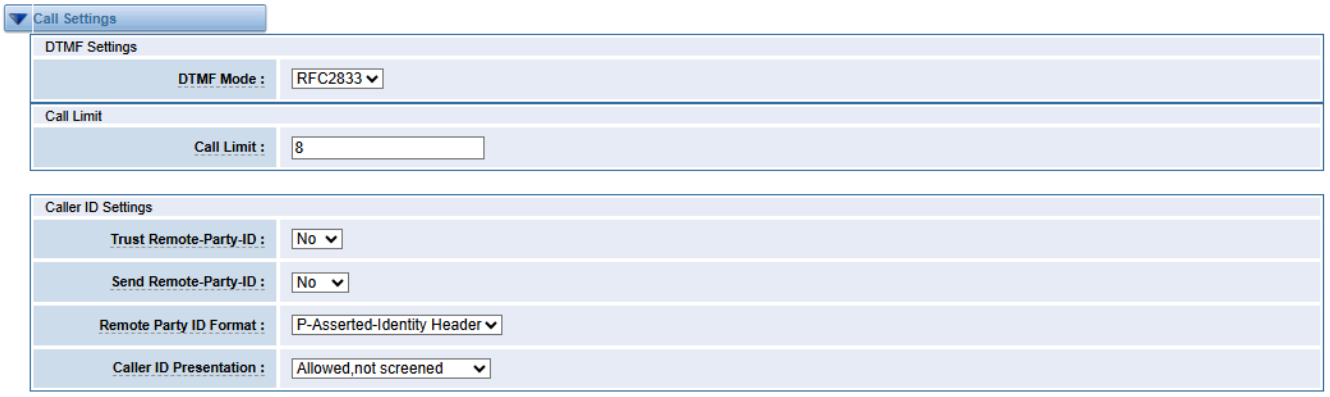
Field Name	Description	Configuration Recommendation
Password	Password used for SIP registration or authentication.	Assigned by the SIP platform and must match the username.
Registration	Sets whether this SIP peer registers with the server.	For a registration-based SIP server, registration is usually enabled. For point-to-point interconnection or trunk mode, set it to None or another mode according to the actual scenario.
Domain Name or IP Address	Domain name or IP address of the primary SIP server.	Enter the primary server address, such as the public IP address or domain name of the SIP server.
Backup Domain Name or IP Address	Backup server address used when the primary server is unreachable.	Recommended when primary and backup servers are deployed to improve reliability.
Port	SIP server listening port.	Common values are 5060 (UDP/TCP) or 5061 (TLS). It must match the actual server configuration.
Transport	Specifies the transport protocol for SIP signaling.	Common options include UDP, TCP, and TLS. UDP is generally used by default. Select TLS if the platform requires encrypted transport.
NAT Traversal	Improves SIP communication when the device is deployed behind NAT.	Recommended when the device is deployed in a private network and accesses the Internet through a router.
Subscribe MWI	Sets whether to subscribe to MWI (Message Waiting Indicator) messages.	Enable it if the platform supports voicemail and message waiting status must be displayed; otherwise, disable it.
VOS Encryption	Sets whether to enable VOS-related encryption.	Enable only according to peer platform compatibility requirements. Do not enable it if the peer does not support it.
STUN Switch	Enables or disables STUN to assist address discovery in NAT environments.	Enable it in complex NAT environments together with server requirements. If another NAT traversal solution is available, keep it disabled.
Priority Match	Controls the priority policy of the current SIP peer during route matching or incoming call identification.	When multiple SIP peers exist and a specific line must be matched first, enable it as needed.

4.1.2 Advanced: Registration Selection



Parameter Name	Description	Recommended Configuration
Authentication User	Set the username used for registration authentication.	Enter the authentication account provided by the platform.
Registration Extension	Set the extension number used during registration.	Fill in this field when an independent extension is required.
Registration Username	Set the SIP registration username.	Keep it consistent with the platform registration account.
User Source	Set the user field source or customized user identity.	Keep the default setting if there are no special requirements.
Domain From	Set the registration domain source.	Enter the domain according to platform requirements.
Authentication	Set whether to enable registration authentication.	Enabling it is generally recommended.
Detection Frequency	Set the registration status detection period.	Keep the default value.
External Proxy	Set the external SIP proxy address and port.	Configure when required by the platform.
Custom Registration Switch	Enable or disable custom registration logic.	Keep OFF if there are no special requirements.
Enable outboundproxy to Replace Host	Set whether to replace Host with the proxy address.	Enable only when explicitly required by the peer.

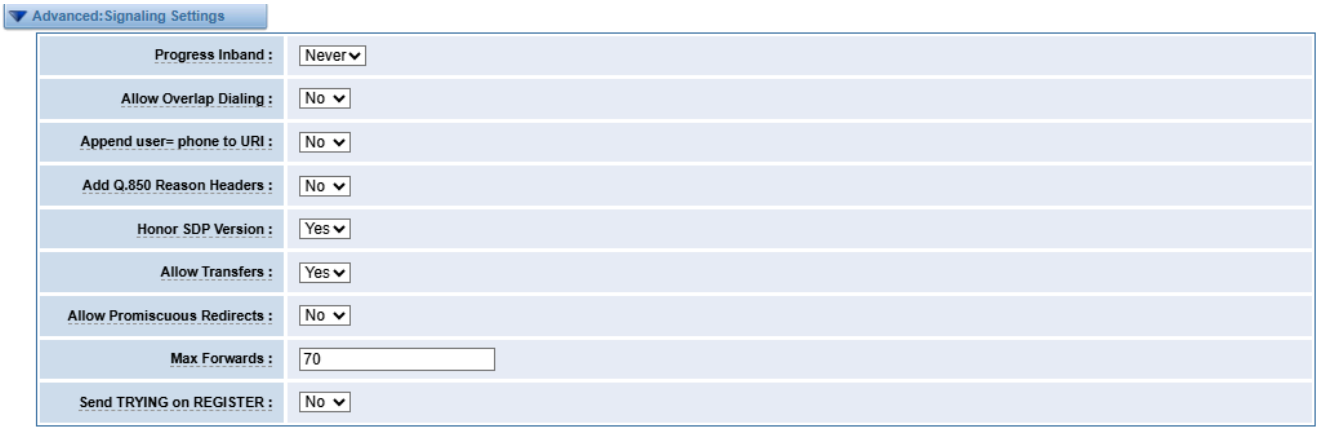
4.1.3 Call Settings



Parameter Name	Optional Value	Description	Recommended Configuration
DTMF Mode	RFC2833 / Inband / Info	Set the DTMF transmission mode.	RFC2833 is recommended first.
Call Limit	Custom value	Set the maximum number of allowed concurrent calls.	Set according to line capacity.
Trust Remote-Party-ID	Yes / No	Set whether to trust caller number information sent by the peer.	Enable when the peer is trusted.
Send Remote-Party-ID	Yes / No	Set whether to send Remote-Party-ID caller information to the peer.	Enable when required by the peer.
Peer Party ID Format	P-Asserted-Identity Header / Remote-Party-ID Header	Set the SIP header format used for caller identity transfer.	P-Asserted-Identity Header is generally preferred.
Caller ID Description	Allowed, not screened	Allows the caller number and does not screen it.	Common default option.
Caller ID Description	Allowed, passed screen	Allows the caller number but requires it to match screening rules.	Applicable when numbers must be released according to rules.
Caller ID Description	Allowed, failed screen	The current number failed screening but is still in an allowed state.	Test and confirm before use.
Caller ID Description	Allowed	Allows the caller number.	Applicable to common scenarios.
Caller ID Description	Prohibited, not screened	Prohibits use of the caller number and does not screen it.	Applicable when number release is prohibited.

Parameter Name	Optional Value	Description	Recommended Configuration
Caller ID Description	Prohibited, passed screen	Prohibits use even if screening is passed.	Used in strict restriction scenarios.
Caller ID Description	Prohibited, failed screen	Failed screening and prohibited.	Used in strict restriction scenarios.
Caller ID Description	Prohibited	Prohibits use of the caller number.	Use when the peer does not allow customized caller ID.
Caller ID Description	Unavailable	Current caller information is unavailable.	Check the configuration source.

4.1.4 Advanced: Signaling Settings

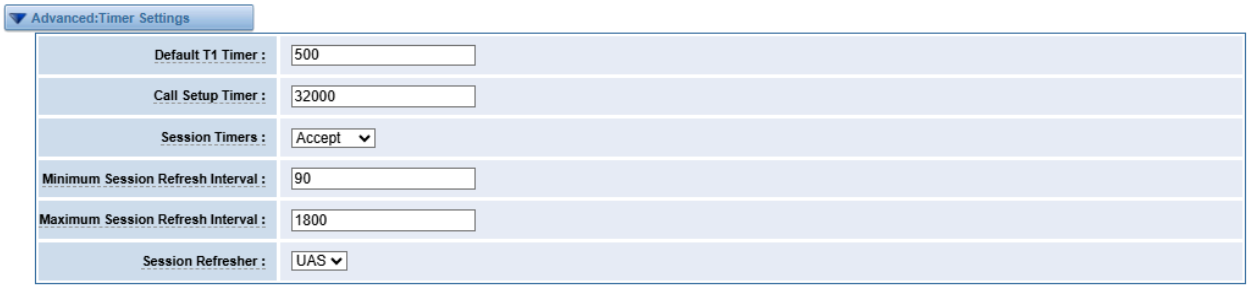


Function Module	Configuration Item	Optional Value / Example Value	Description	Recommendation
Advanced Signaling Settings	Incoming Inband Signaling	Never (current UI value) / other vendor-defined options	Controls whether inband signaling tones, such as ringback tone, busy tone, or other prompt tones, are provided to the peer in incoming call scenarios. Available values may vary slightly by device version.	Keep the default setting if the peer platform or service scenario has no special requirements. Adjust according to peer requirements for early media or special prompt tone scenarios.
Advanced Signaling Settings	Allow Duplicate Dialing	Yes / No	Controls whether duplicate numbers or duplicate destination codes are allowed during dialing.	Configure according to live network service requirements. Set to No if repeated call attempts must be avoided.

Function Module	Configuration Item	Optional Value / Example Value	Description	Recommendation
Advanced Signaling Settings	Add User=Phone to URI	Yes / No	Controls whether the user number is appended to the SIP URI. This is often used for number identification or route matching with the peer platform.	Enable if the peer platform has explicit requirements for the user number in Request-URI or To/From. Otherwise, keep the default setting.
Advanced Signaling Settings	Add Q.850 Reason Header	Yes / No	Adds Q.850 cause codes in SIP signaling, which helps when connecting to traditional voice networks, carrier platforms, or systems requiring clear release causes.	Recommended when connecting to softswitches, carrier platforms, or scenarios requiring accurate fault location.
Advanced Signaling Settings	SDP Version Header	Yes / No	Controls whether SIP/SDP messages carry or update SDP version-related fields.	Keep the default setting in most cases. If the peer strictly validates SDP negotiation, adjust according to peer requirements.
Advanced Signaling Settings	Allow Call Transfer	Yes / No	Controls whether call transfer is allowed through SIP REFER and similar methods.	Enable when call transfer service is required. Disable if only basic trunk connection is used.
Advanced Signaling Settings	Allow Source Redirect	Yes / No	Controls whether source address-related redirection processing is accepted or initiated. This is usually related to 3xx responses or route redirection mechanisms.	Enable if the network structure is complex and redirection routing is required. If there are no special requirements, disable it.
Advanced Signaling Settings	Max Forwards	Numeric value, for example 70	Limits the maximum number of times a call can be forwarded, redirected, or transferred to prevent call loops.	Keep a reasonable default value and avoid setting it too high.

Function Module	Configuration Item	Optional Value / Example Value	Description	Recommendation
Advanced Signaling Settings	Send TRYING for Registration	Yes / No	Controls whether the device sends TRYING responses or related processing messages during registration or related transactions. The specific behavior may depend on device implementation.	Keep the default setting if the peer platform has no special requirements. For registration interaction with specific platforms, adjust according to test results.

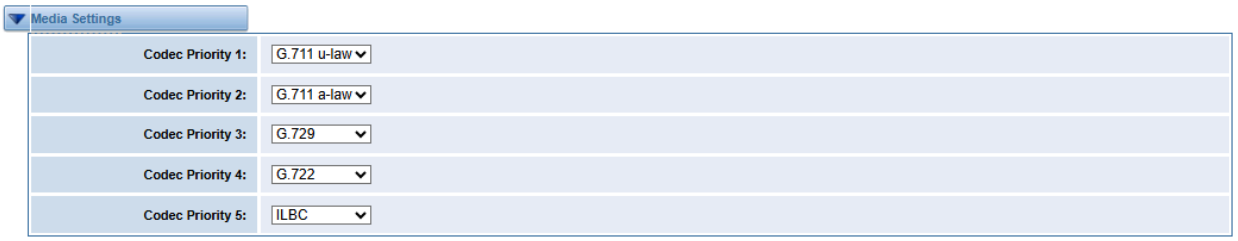
4.1.5 Advanced: Timer Settings



Function Module	Configuration Item	Optional Value / Example Value	Description	Recommendation
Advanced Timer Settings	Default T1 Timer	Numeric value, for example 500	Sets the base time unit of SIP transaction timer T1. T1 is commonly used as the reference time for request retransmission and transaction timeout.	Keep the default value unless peer network latency is high or the vendor provides explicit adjustment requirements.
Advanced Timer Settings	Call Setup Timer	Numeric value, for example 32000	Controls timeout during the call setup phase. If the call is still not established after the configured time, the system can determine that this call setup failed.	Keep the default setting. Increase it as needed in cross-region, high-latency networks or special interconnection scenarios.

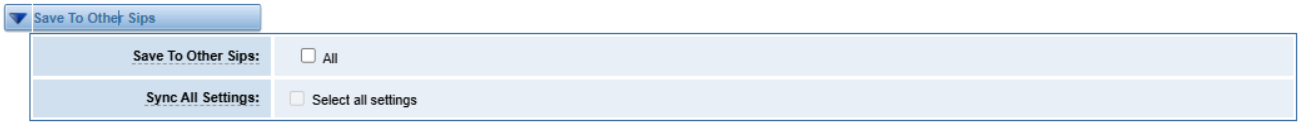
Function Module	Configuration Item	Optional Value / Example Value	Description	Recommendation
Advanced Timer Settings	Session Timer	Accept (current UI value) / other options	Controls how the device handles the SIP Session Timer mechanism, such as whether to accept session timer refresh.	If the peer platform supports Session Timer, keep the default Accept setting or configure according to peer requirements.
Advanced Timer Settings	Minimum Session Refresh Interval	Numeric value, for example 90	Defines the minimum allowed session refresh interval to prevent refreshes from being too frequent and increasing system load.	Keep the default value and avoid setting it too low.
Advanced Timer Settings	Minimum Session Refresh Interval	Numeric value, for example 1800	Based on the UI value, this item is more likely used to control the session refresh period, session expiration time, or maximum session interval.	Use the default value and configure it together with the peer Session-Expires negotiation mechanism.
Advanced Timer Settings	Session Refresher	UAS (current UI value) / other options	Specifies which side initiates session refresh. UAS means the called-side server/device is responsible for refresh and affects Session Timer negotiation behavior.	Configure according to peer specifications if the peer platform has explicit requirements. Otherwise, keep the default setting.

4.1.6 Media Settings



Function Module	Configuration Item	Optional Value / Example Value	Description	Recommendation
Codec Settings	Highest Priority Codec 1	G.711 u-law	Sets the first-priority codec for voice negotiation. A higher priority codec participates earlier in SIP/SDP media negotiation.	G.711 u-law is preferred in North America, Japan, or scenarios requiring high compatibility.
Codec Settings	Highest Priority Codec 2	G.711 a-law	Sets the second-priority codec for voice negotiation.	G.711 a-law is common in China, Europe, and most carrier voice network scenarios.
Codec Settings	Highest Priority Codec 3	G.729	Sets the third-priority codec for voice negotiation. G.729 uses low bandwidth and is suitable for bandwidth-limited scenarios.	Enable it when link bandwidth is limited and voice traffic compression is required.
Codec Settings	Highest Priority Codec 4	G.722	Sets the fourth-priority codec for voice negotiation. G.722 supports wideband voice and usually provides better quality than traditional narrowband codecs.	Applicable to HD voice scenarios, but confirm peer support first.
Codec Settings	Highest Priority Codec 5	iLBC	Sets the fifth-priority codec for voice negotiation. iLBC has some packet loss resistance.	Applicable to unstable network quality scenarios, but confirm peer compatibility first.
Save to Other SIP	Synchronize All Settings	Checked / Select all	Synchronizes all related settings on the current page or current object to other SIP configurations.	Can be used for batch deployment. Before operation, confirm whether target SIP configurations need to be fully overwritten.

4.1.7 Save to Other SIP



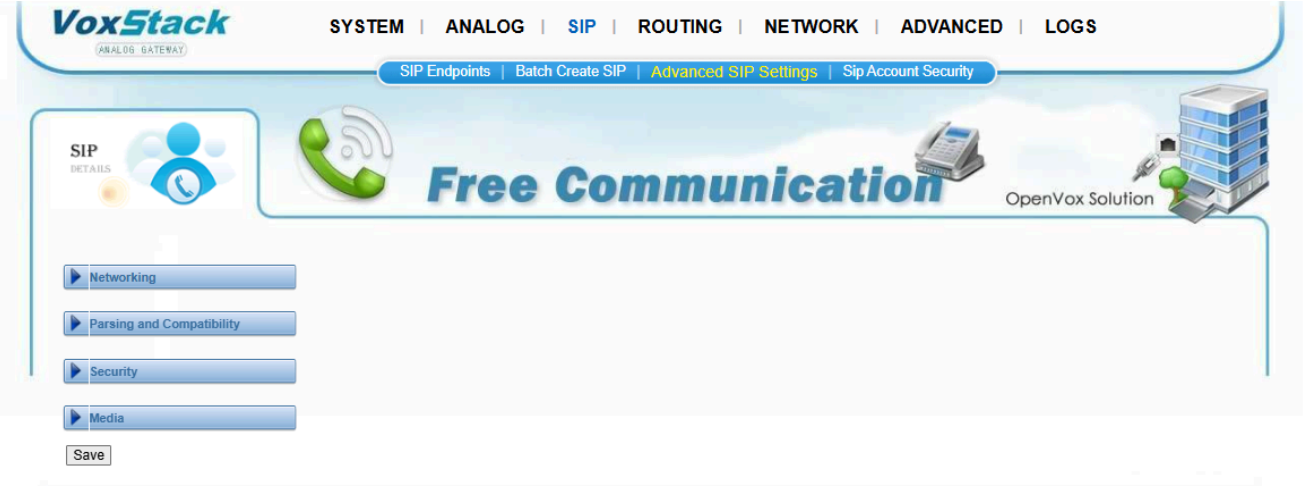
Parameter Name	Description	Value Description	Configuration Recommendation
Save to Other SIP	Apply the current configuration to other SIP items in batches.	Checked / Select all.	Use for batch deployment.
Synchronize All Settings	Synchronize all current settings to other SIP items.	Checked / Select all.	Confirm target configurations before overwriting.

4.2 Batch Create SIP Accounts

The SIP Endpoint page is used to configure SIP account information for the gateway device, enabling registration and communication between the device and a SIP server, IPPBX, or carrier platform. On this page, users can configure the username, password, server address, port, registration mode, and other parameters separately for each SIP port or account. When the device needs to connect to multiple SIP accounts, users can centrally manage them in list mode and improve deployment efficiency with the batch settings function. After configuration is completed and saved, the device registers with the corresponding SIP platform according to the entered parameters for subsequent call connection and voice service communication.

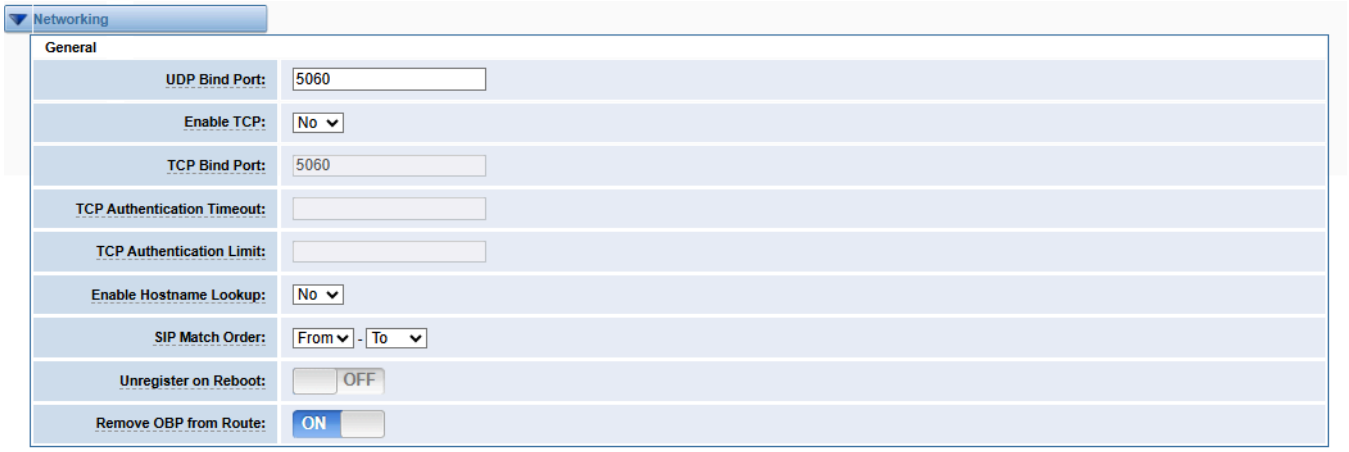
4.3 Advanced Settings

This section is mainly used to configure advanced SIP parameters, including network, compatibility, security, and media-related options. It is generally recommended to adjust these settings according to peer platform requirements only after basic registration and calls work normally.



4.3.1 Networking

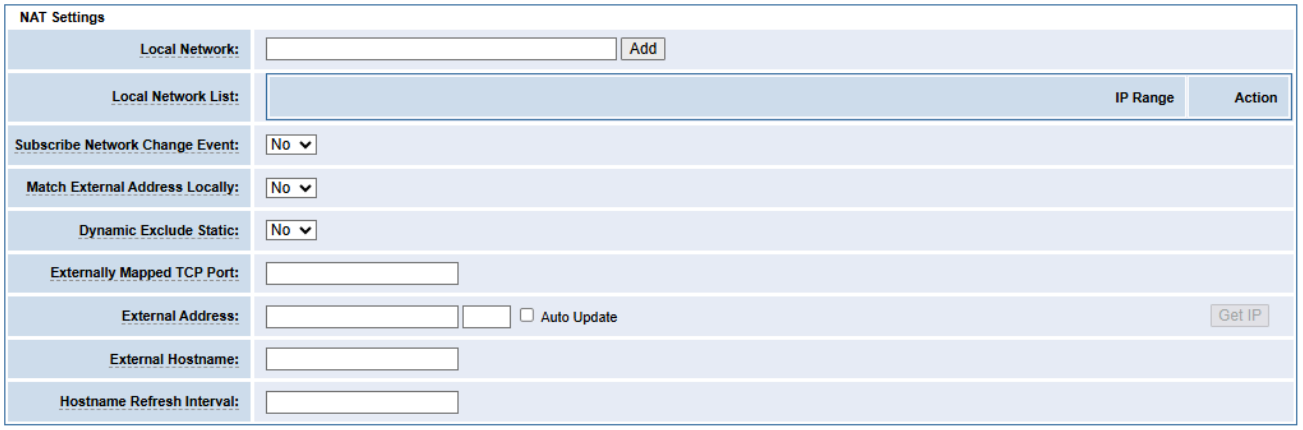
(1) General



Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
UDP Binding Port	5060	Sets the local listening port used by SIP over UDP for sending and receiving SIP signaling messages such as registration and calls.	Generally keep the default 5060. Modify it as needed if there is a port conflict.
Enable TCP	Yes / No	Sets whether SIP signaling is transmitted over TCP.	Enable when required by the peer platform. Otherwise, usually disable it.
TCP Binding Port	5060	Sets the local listening port used by SIP over TCP.	Configure as needed when TCP is enabled. Usually keep the default value.
TCP Authentication Timeout	Numeric value	Sets timeout for TCP authentication or connection-related processing.	Keep the default setting. Adjust as needed in special network environments.

Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
TCP Authentication Limit	Numeric value	Sets TCP authentication count or authentication limit parameters.	Use the default value.
Enable Hostname Lookup	Yes / No	Sets whether DNS lookup is allowed for SIP server addresses.	Recommended when registering by domain name.
SIP Match Order	From / To	Sets the matching order of related headers when the system processes SIP messages.	Keep the default setting if there are no special requirements.
Unregister on Reboot	ON / OFF	Sets whether the device actively sends an unregister message to the SIP platform before rebooting.	Generally keep the default. Enable it if the peer requires standard unregister behavior.
SIP Remove External Proxy Route	ON / OFF	Sets whether to remove route information related to the external proxy from SIP messages.	Enable it when the peer platform is sensitive to Route headers.

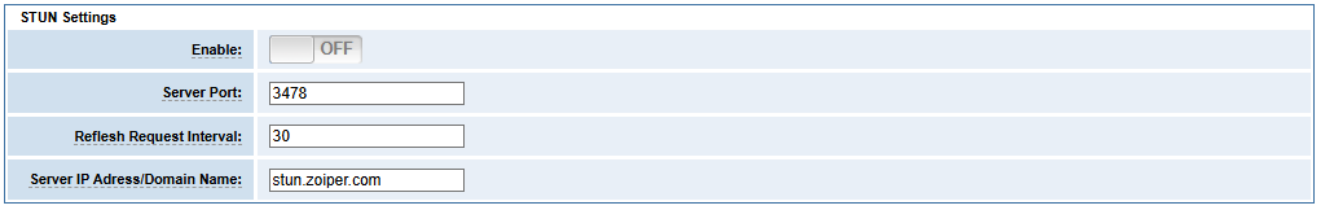
(2) NAT Settings



Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Local Network	Network segment/IP, for example 192.168.1.0/24	Defines the local network address range to help the device identify intranet addresses.	Correctly fill in the local subnet in NAT environments.

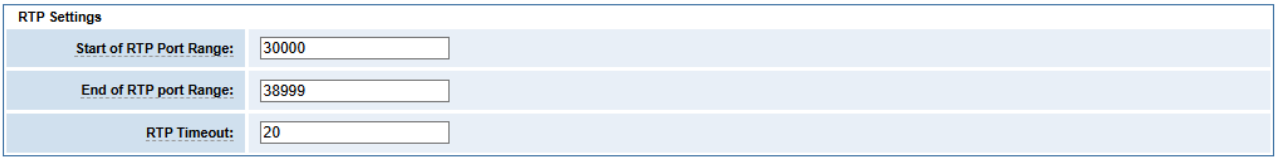
Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Local Network List	List item	Displays and manages added local network ranges.	Add items one by one if there are multiple intranet subnets.
Subscribe Network Change Time	Yes / No	Sets whether the device detects or subscribes to network address changes.	Enable it when the network environment may change.
Local Match External Address	Yes / No	Sets whether local and external addresses are mapped and matched.	Enable as needed in NAT traversal scenarios.
Dynamic and Static Selection	Yes / No	Sets whether the external address is obtained dynamically or configured statically.	Use static for fixed public IP. Use automatic update for dynamic public IP.
External TCP Port Mapping	Numeric value	Sets the externally announced TCP port mapping value after NAT.	Fill in this field when the external mapped port is different from the local port.
External IP Address	IP address / Auto Update	Sets the public IP address announced by the device in SIP/SDP.	Enter it manually for a fixed public IP. Enable automatic update for a dynamic public IP.
External Hostname	Domain name	Sets the hostname used externally by the device.	Enter this field when using DDNS or a public domain name.
Hostname Refresh Interval	Numeric value	Sets the refresh period for the external hostname or public address.	Configure as needed for dynamic public address scenarios.

(3) STUN Settings



Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Enable	ON / OFF	Sets whether to enable STUN, which is used to discover public addresses and ports behind NAT.	Enable when the device is behind NAT.
Server Port	3478	Sets the port number used by the STUN server.	Generally keep the default 3478.
Refresh Request Interval	30	Sets the interval for sending refresh requests to the STUN server.	Keep the default value.
Server IP Address / Domain Name	stun.zoiper.com	Sets the STUN server address used to obtain public mapping information.	Use an available STUN server or configure according to platform requirements.

(4) RTP Settings

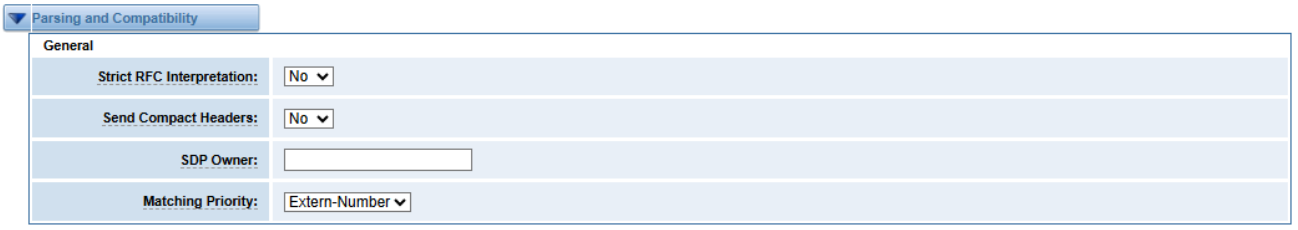


Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Start RTP Port	30000	Sets the starting port number used by RTP voice media streams. After a call is established, the device allocates ports from this range for voice data transmission.	Plan this together with firewall policies and avoid conflicts with other service ports.
End RTP Port	38999	Sets the ending port number used by RTP voice media streams. Together with the start port, it defines the available RTP port range.	Set a reasonable port range based on concurrent call quantity and ensure the corresponding ports are allowed on the network side.

Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
RTP Timeout	20	Sets timeout judgment time when no RTP media stream data is received. After this time, the system can treat the media stream as abnormal or interrupted.	Keep the default value in most cases. Adjust according to site conditions when network jitter is high.

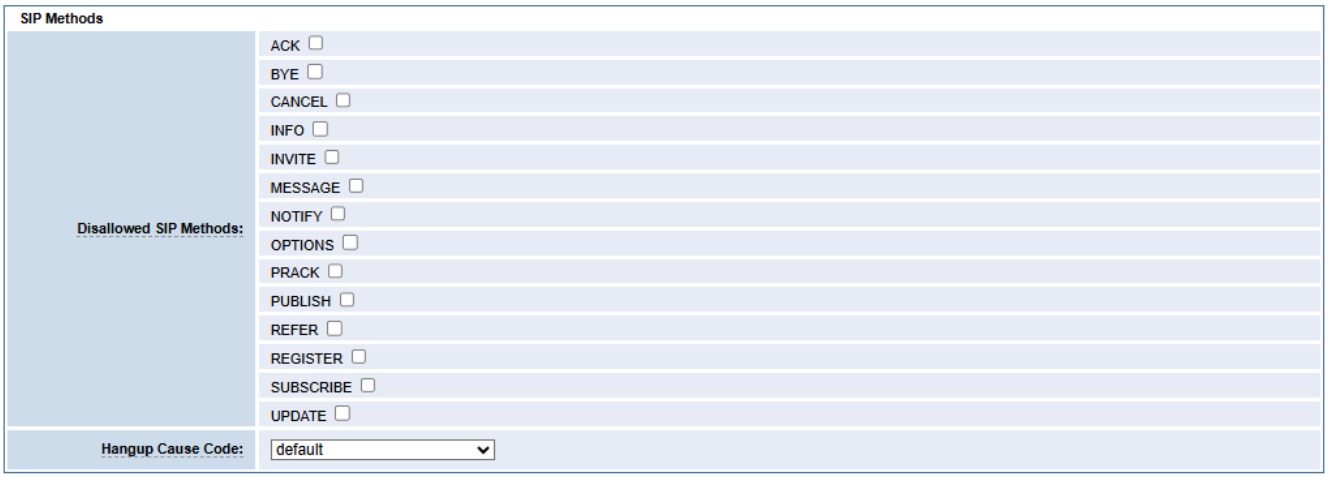
4.3.2 Parsing and Compatibility

(1) General



Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Strict RFC Parsing	Yes / No	Sets whether the device parses SIP messages according to stricter RFC specifications. After this option is enabled, tolerance for non-standard SIP messages is reduced.	Enable when connecting to a standard SIP platform. If peer compatibility is poor, configure based on actual test results.
Send Compact Header	Yes / No	Sets whether to send compact SIP headers, such as using abbreviated headers instead of full standard headers.	Disable if there are no special requirements to make packet capture analysis easier and improve compatibility.
SDP Owner	Custom string	Sets content related to the owner field in SDP, used to identify the session originator during media negotiation.	Keep the default setting. Modify only when the peer has special SDP validation requirements.
Match Priority	Called number (UI example)	Sets the priority basis used by the system for number matching, route judgment, or account matching.	Keep the default setting if there are no special requirements. Adjust if the site matches by caller number or another field.

(2) SIP Methods

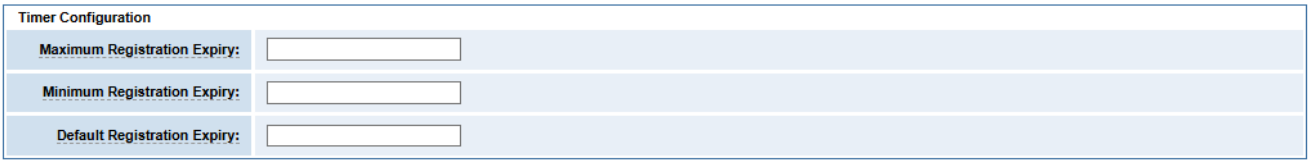


Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Disallow SIP Methods	ACK / BYE / CANCEL / INFO / INVITE / MESSAGE / NOTIFY / OPTIONS / PRACK / PUBLISH / REFER / REGISTER / SUBSCRIBE / UPDATE	Used to restrict the device from receiving or processing certain SIP methods. After selected, the system can reject corresponding types of SIP requests.	Do not arbitrarily restrict common methods. Configure only when security control or peer compatibility requirements are clear.
Hangup Cause Code	Default	Sets the SIP hangup cause code policy returned when a call is released.	Keep the default setting if there are no special requirements.

(3) Caller Number and Called Number

Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Shrink Caller ID	Yes / No	Sets whether the caller number is shortened, trimmed, or compressed in format.	Enable only when the peer platform has requirements for caller number length.
SIP From	Name (UI example)	Sets how caller information is presented in the SIP From header.	Keep the default setting in most cases. Modify as needed when the peer requires number-based or username-based display.
Caller Number Settings	ON / OFF	Enables or disables advanced control functions related to caller numbers.	Keep the default setting if there are no special requirements.
SIP To	Tel/Tel (UI example)	Sets the presentation format of called information in the SIP To header.	Configure according to peer platform requirements. Usually the default setting is sufficient.
Called Number	EXTEN (UI example)	Sets the value source or encoding method of the called number field.	Keep the default setting in most cases. Adjust as needed for special routing scenarios.
Allow Empty Called Number	ON / OFF	Sets whether an empty called number is allowed to be sent.	Generally disable it to avoid call failure or peer rejection.

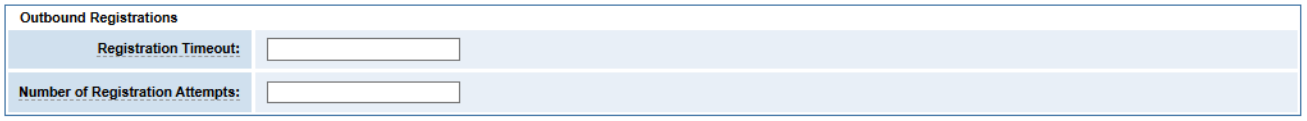
(4) Timer Settings



Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Maximum Registration Timeout	Numeric value	Sets the maximum allowed registration timeout.	Configure according to peer platform registration period requirements.

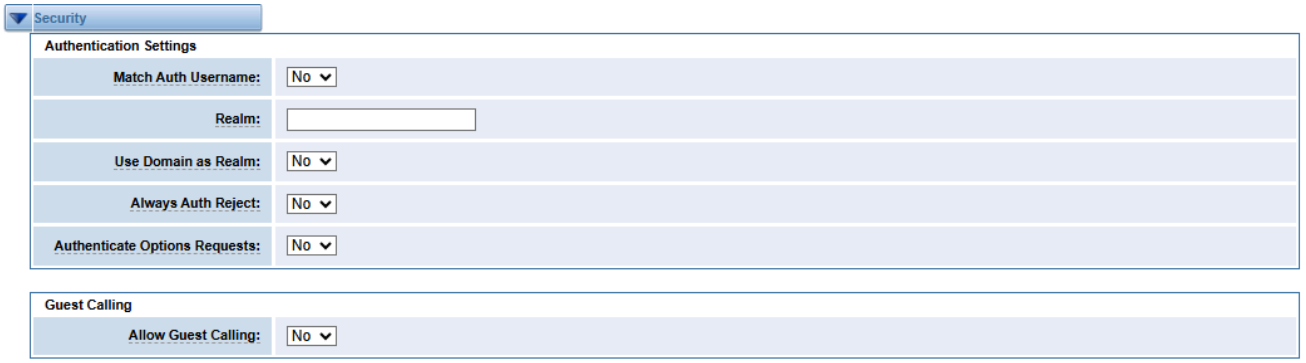
Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Minimum Registration Timeout	Numeric value	Sets the minimum allowed registration timeout.	Do not set it too low to avoid frequent registration.
Default Registration Timeout	Numeric value	Sets the registration timeout used by the device by default.	Configure according to the platform recommended value.

(5) External Registration



Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Registration Timeout	Numeric value	Sets timeout for external registration requests. If no response is received within the configured time, registration can be determined as failed.	Increase as needed when network latency is high.
Registration Attempts	Numeric value	Sets the number of retry attempts after registration failure.	Set reasonably according to network stability and platform limits.

4.3.3 Security



Parameter Name	Description	Recommended Configuration
Match Authentication Username	Set whether to verify the SIP authentication username.	Enable when security requirements are high.

Parameter Name	Description	Recommended Configuration
Domain	Set the domain value used for SIP authentication.	Enter the information provided by the platform.
Use Domain Name as Domain	Set whether to use the domain name as the authentication domain.	Enable when required by the peer.
Keep Authentication Header	Set whether to keep authentication-related headers.	Keep the default setting in most cases.
Authenticate OPTIONS Requests	Set whether to authenticate OPTIONS probe requests.	Enable when stronger security control is required.
Allow Client Calls	Set whether clients are allowed to initiate calls.	Enabling it is generally recommended.

4.3.4 Media

Parameter Name	Description	Recommended Configuration
Early Media	Set whether to transmit ringback tone, busy tone, or prompt tone before the call is answered.	Enable when connecting to carriers or announcement tone scenarios.
Redirect Media Stream	Set whether to redirect media streams.	Keep the default setting in most cases.
SIP Packet TOS	Set network priority for SIP signaling packets.	Configure according to live network QoS policy.
RTP Packet TOS	Set network priority for RTP voice packets.	Configure according to voice priority policy.

4.4 SIP Account Security

This page is used to configure SIP over TLS encrypted transport parameters, including the TLS switch, server certificate verification, TLS port, client mode, and certificate file management. By uploading the corresponding certificate and key files and correctly configuring TLS parameters, encrypted registration and secure communication between the device and the SIP platform can be implemented. During deployment, configure

certificate type, port number, and verification method correctly according to TLS interconnection requirements provided by the peer platform to ensure normal registration and call services.

Parameter Name	Description	Recommended Configuration
Enable	Set whether to enable TLS encrypted transport.	Enable when connecting to a secure platform.
TLS Verify Server	Set whether to verify the peer certificate.	Enable when security requirements are high.
Port	Set the TLS transport port.	5061 is generally used.
TLS Client Mode	Set the TLS protocol mode.	Configure according to the peer supported version.
Type	Set the certificate type.	Client is generally selected.
Key Name	Set the certificate entry name.	Use an easily identifiable name.
IP Address	Set the address associated with the certificate.	Enter the peer server address.
Organization	Set certificate organization information.	Enter the actual information.
Password	Set the certificate or private key password.	Enter the actual file password.
Upload PEM File	Upload a PEM certificate or private key file.	Upload according to platform requirements.

Parameter Name	Description	Recommended Configuration
Upload CRT File	Upload a CRT certificate file.	Upload according to platform requirements.

5. Routing Settings

Go to the `Routing Settings` menu. The routing settings page provides three major configuration sections:

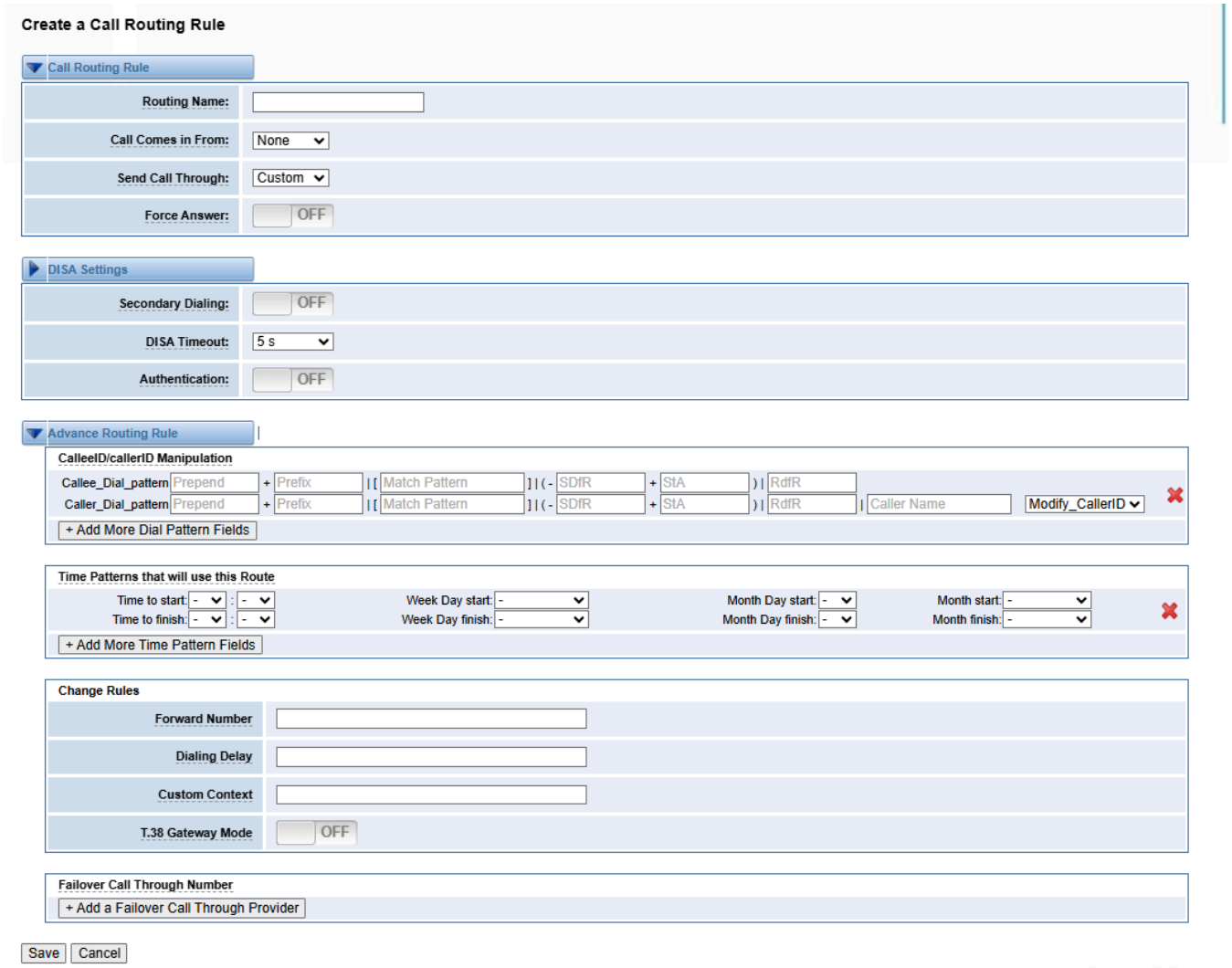
- Add, delete, and sort call routing rules.
- Configure groups.
- Batch create call routing rules.

5.1 Call Routing Rules

This page is mainly used to configure call routing rules, including incoming and outgoing call forwarding, matching, transformation, and failure handling logic. Before deployment, confirm call ingress, call egress, and number processing rules.

Add Call Routing Rule

This page is used to configure call routing rules for the gateway device, including call source, call destination, DISA secondary dialing, number filtering and transformation, time-based effective conditions, and handling policy after call failure. On this page, users can flexibly configure incoming and outgoing call handling logic according to different service scenarios, such as forwarding by source, distributing by time period, rewriting by number rules, and rerouting after failure. During deployment, confirm call ingress, egress, and number format requirements first, and then plan time policies and exception handling mechanisms in a unified way.



The configuration items in the figure above are described in the following tables.

(1) Call Routing Rule

Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Route Name	Custom string	Sets the name of the current call routing rule to distinguish and manage different routes.	Use a meaningful service name, such as "FXS to SIP" or "Incoming to Extension".
Call From	None / specific port/SIP/GROUP	Sets the call source of this route, meaning which interfaces, accounts, or objects enter this route.	Select the source according to the actual inbound direction.
Call To	Custom / other target object	Sets the call destination of this route, meaning where the call is forwarded after the rule is matched.	Configure according to the actual outbound direction or service target.

Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Forced Answer on Reject	ON / OFF	Sets whether the system executes forced-answer processing logic when the target side rejects the call.	Keep the default setting if there are no special service requirements.

(2) DISA Settings

Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Secondary Dialing	ON / OFF	Sets whether to enable DISA secondary dialing. After enabled, an incoming call can continue entering numbers for a second call.	Enable when DISA external access or secondary dialing service is required.
DISA Timeout	5 s	Sets the timeout for DISA to wait for user number input.	Configure according to actual dialing habits. 5 seconds or longer is commonly used.
Verification	ON / OFF	Sets whether DISA requires identity verification. If enabled, the maximum password length and customized password can be configured.	To prevent unauthorized access, enable verification when DISA is enabled.

(3) Advanced Routing Rules

Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Caller/Called Number Filtering and Transformation	Add prefix / delete digits / retain digits / matching string / caller name / Modify_CallerID	Used to match, filter, truncate, pad, add prefixes, and modify caller names for caller or called numbers.	Use when the peer platform has number format requirements. Test before going live.
Time Pattern for This Rule	Start time / end time / start weekday / end weekday / start date / end date / start month / end month	Defines the effective time range of the current routing rule to implement time-based routing.	Applicable to scenarios such as work-hour and non-work-hour routing.

Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Add Routing Rule	Button operation	Adds a new number processing rule.	Use when multiple number processing logic items are required.
Add Time Pattern	Button operation	Adds a new time-based effective condition.	Use when multiple effective time periods are required.

(4) Change Status Rules

Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Forward Number	Custom string	Sets the target number used for call forwarding.	Enter the actual forwarding target.
Dialing Delay	Numeric value	Sets the dialing wait time before executing the routing action.	Keep the default setting or leave it blank if there are no special requirements.
Custom Dial Rule Context	Custom string	Sets the context used by customized dial plans or dialing rules.	Configure only when connecting to a customized dial rule environment.
T.38 Gateway Mode	ON / OFF	Sets whether to enable T.38 fax gateway mode. After enabled, the device can perform T.38-related processing for fax services.	Enable when fax service is involved. Otherwise, usually disable it.

(5) Call Failure Handling

Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Add Call Failure Handling	Button operation	Adds handling logic after call failure, such as rerouting to another route, forwarding, or executing another service policy.	Configure a backup route after failure for key services.

5.2 Groups

This page is mainly used to create and manage routing groups so multiple objects can participate in call distribution under a unified policy. For scenarios requiring multi-line polling or sequential outbound calling, use the group function first.

Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Group Description	Custom string	Sets the name or description of the routing group to identify its purpose. The UI indicates that letters, digits, and some special characters can be used, with a maximum length of 32 characters.	Use a meaningful service name, such as "SIP Outbound Group" or "Extension Transfer Group".
Type	SIP / MAG	Sets the object type of the current routing group. Different types usually correspond to different interfaces or resource objects. If MAG is selected, multiple Magnet interfaces can be customized as one group, and all Magnet interfaces can also be used as a single group.	Configure according to actual resource type.

Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
Policy	Ascending / descending / polling / reverse polling	Sets the call distribution or selection policy for group members. Ascending usually means trying members in order.	Use ascending if there are no special requirements. Select polling or another distribution mode as required by the service.
Members	NO. / All	Sets the member objects added to the current group. Members can be selected individually or all at once.	Select group members according to actual service needs and avoid accidentally selecting all objects.

5.3 Batch Create Call Routing Rules

This page is mainly used to generate call routing rules in batches, which applies to multi-port unified deployment scenarios. Confirm the correspondence between ports, numbers, and trunks before running batch configuration.

Parameter Name	Description	Recommended Configuration
Port	Select the port that needs routing rule configuration.	Configure according to actual service ports.
Forward Number	Set the forwarding target number for the port.	Use auto-increment for consecutive number scenarios.

Parameter Name	Description	Recommended Configuration
SIP Trunk	Set the SIP trunk line used by the port.	Select according to actual trunk resources.
Caller Extension Number	Set the extension number displayed or used externally by the port.	Use auto-increment for consecutive extension scenarios.
Auto-Increment	Automatically generate numbers in sequence.	Use for consecutive numbering scenarios.
Copy	Copy the same value to multiple ports.	Use when the same configuration is required.
Batch Settings (Auto-Increment)	Generate consecutive configurations in batches.	Use for multi-port batch deployment.
Batch Settings (Copy)	Copy identical configurations in batches.	Use for unified configuration.

6. Network Configuration

Go to the `Network Configuration` menu. The network configuration page includes basic settings, VPN settings, DDNS settings, tools, security settings, firewall security rules, and static routing settings.

- Add, delete, and sort call routing rules.
- Configure groups.
- Batch create call routing rules.

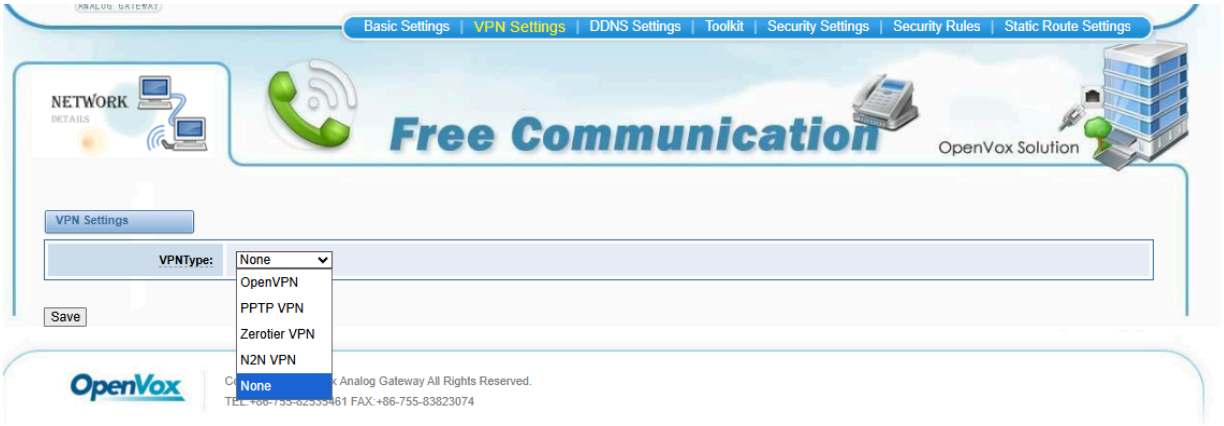
6.1 Basic Settings

This page is mainly used to configure basic network parameters of the device, including IP address, subnet mask, default gateway, and DNS. To ensure stable management and service communication later, using a fixed IP address is recommended.

Parameter Name	Description	Recommended Configuration
Network Mode	SWITCH	Currently, only switch mode is supported.
Type	Factory / Static / Dynamic Host Configuration - Factory: 172.16.80.X, where X depends on the UCP slot number - Static: custom address/subnet mask/default gateway can be configured - Dynamic Host Configuration: DNS/DHCP must be associated to provide IP allocation	It is recommended to change this to Static and enter an unused IP address in the local network segment.
Physical Address	Displays the NIC MAC address.	No modification is required.
Address	Sets the LAN2 IP address.	Enter it according to intranet planning.
Subnet Mask	Sets the LAN2 subnet mask.	Enter it according to subnet planning.

Parameter Name	Description	Recommended Configuration
Default Gateway	Sets the LAN2 default gateway.	Enter it when cross-subnet communication is required.
Type	Sets the DNS server method.	Manual DNS can generally be used.
Domain Name Server 1	Sets the primary DNS.	Enter a commonly available DNS server.
Domain Name Server 2	Sets the backup DNS.	Enter a backup DNS server.
Enable	Sets whether to enable the preset access IP address.	Enable when a backup access address is required.
Preset Address	Sets the backup access IP address.	Enter it according to the management network segment.
Preset Subnet Mask	Sets the backup access subnet mask.	Keep it consistent with the preset address.

6.2 VPN Settings



Parameter Name	Optional Value / Example Value	Description	Configuration Recommendation
VPN Type	OpenVPN / PPTP VPN / Zerotier VPN / N2N VPN / None	Used to select the VPN working type of the device. Different types correspond to different tunnel setup methods and networking schemes.	Select None if VPN is not required. If remote networking or cross-subnet access is required, select the corresponding VPN type according to the site plan.

6.3 DDNS Settings

This page is mainly used to configure DDNS (Dynamic Domain Name System). When the public IP address changes dynamically, the device can still be accessed continuously through a domain name.

This page is used to configure the DDNS (Dynamic Domain Name System) function of the device. When the public IP address of the network environment where the device is located changes, the system can automatically update the latest IP address to the specified domain record, ensuring that users can always access the device through a fixed domain name. During deployment, if the device is located in a dynamic public IP environment and remote access is required, correctly configure the DDNS service type, account information, and target domain name.

Parameter Name	Description	Recommended Configuration
Dynamic Domain Name	Set whether to enable DDNS.	Enable in dynamic public IP scenarios.
Type	Set the DDNS service type.	Select according to service provider requirements.
Username	Set the DDNS account.	Enter the registered account.
Password	Set the DDNS password.	Enter the actual password.
Domain	Set the domain name to bind.	Enter a valid DDNS domain name.

6.4 Tools

This page is mainly used for network diagnosis and packet capture analysis. It can help troubleshoot connectivity, routing exceptions, and SIP communication issues. It is recommended for site debugging and fault location.

Parameter Name	Description	Recommended Configuration
Target Address	Set the domain name or IP address to test.	Enter the SIP server or a public network address.
Ping	Test whether the target is reachable.	Use first for connectivity checks.
Traceroute	View the routing path to the target address.	Use when troubleshooting routing exceptions.
Source Host Address	Set packet capture source address filtering.	Enter it when troubleshooting communication from a specified source address.
Destination Host Address	Set packet capture destination address filtering.	Enter it when troubleshooting specified destination communication.
Port	Set packet capture port filtering.	Common SIP ports are 5060/5061.
Tcpdump Option Parameters	Set advanced packet capture parameters.	Use when there are clear packet capture requirements.
Start	Start diagnosis or packet capture.	Execute after confirming parameters.

6.5 Security Settings

This page is mainly used to configure basic security policies of the device, including firewall, Ping response, whitelist, and blacklist functions. For public network deployment, apply unified settings according to project security requirements.

Configure the basic firewall and access control functions of the device, including firewall switch, Ping response control, whitelist, and blacklist mechanisms. Through these settings, users can apply basic restrictions to the device network access range, reducing unauthorized access and network probing risks. During deployment, enable firewall, whitelist, and blacklist functions reasonably according to site security policies, and decide whether to allow the device to respond to Ping requests according to operation and maintenance requirements.

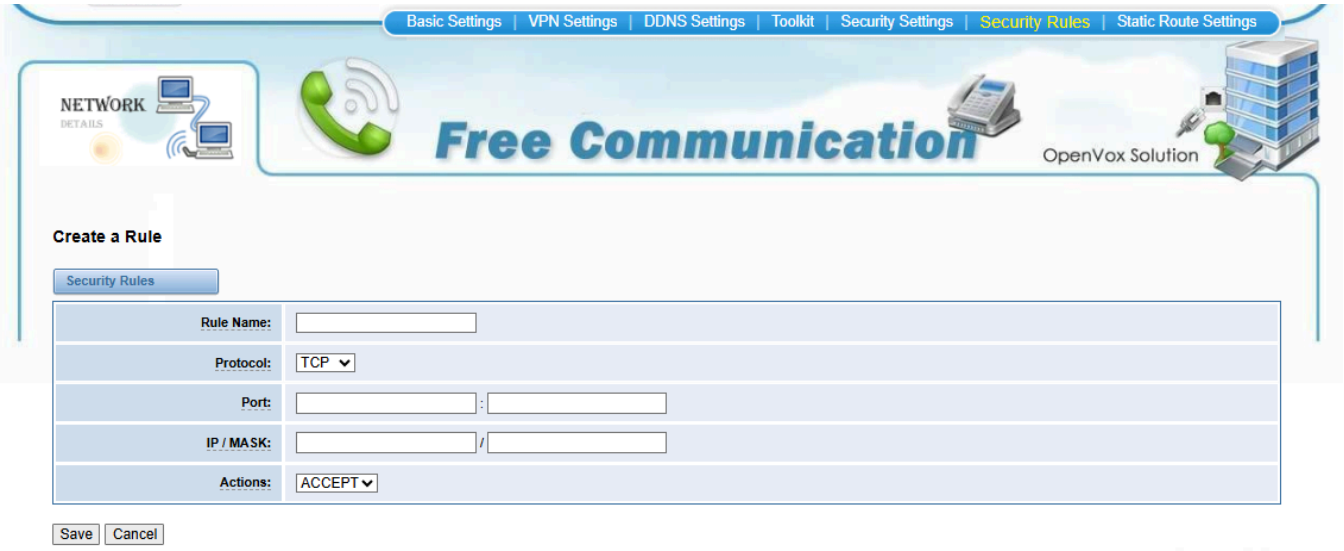
Parameter Name	Description	Recommended Configuration
Firewall Switch	Set whether to enable the device firewall. Blacklist and whitelist can be configured only after the firewall is enabled.	Enabling it is generally recommended.
Ping Switch	Set whether to respond to Ping requests.	Disable as needed in public network environments.
Whitelist Switch	Set whether to enable whitelist access control.	Enable in high-security scenarios.
Blacklist Switch	Set whether to enable blacklist access control.	Enable when specific sources must be blocked.

6.6 Firewall Security Rules

This page is mainly used to add and manage firewall access rules to control access behavior for different protocols, ports, and address ranges. During configuration, allow necessary service ports first and restrict unauthorized access.

Click `New Rule`. The interface is shown below.

This function is used to create firewall security rules, controlling network access behavior by specifying protocol, port range, and address range. Users can configure allow or restrict rules for different types of service traffic according to site security policies, improving device access control. During deployment, allow necessary service ports and legitimate source addresses first, and restrict unnecessary network access to reduce security risks.

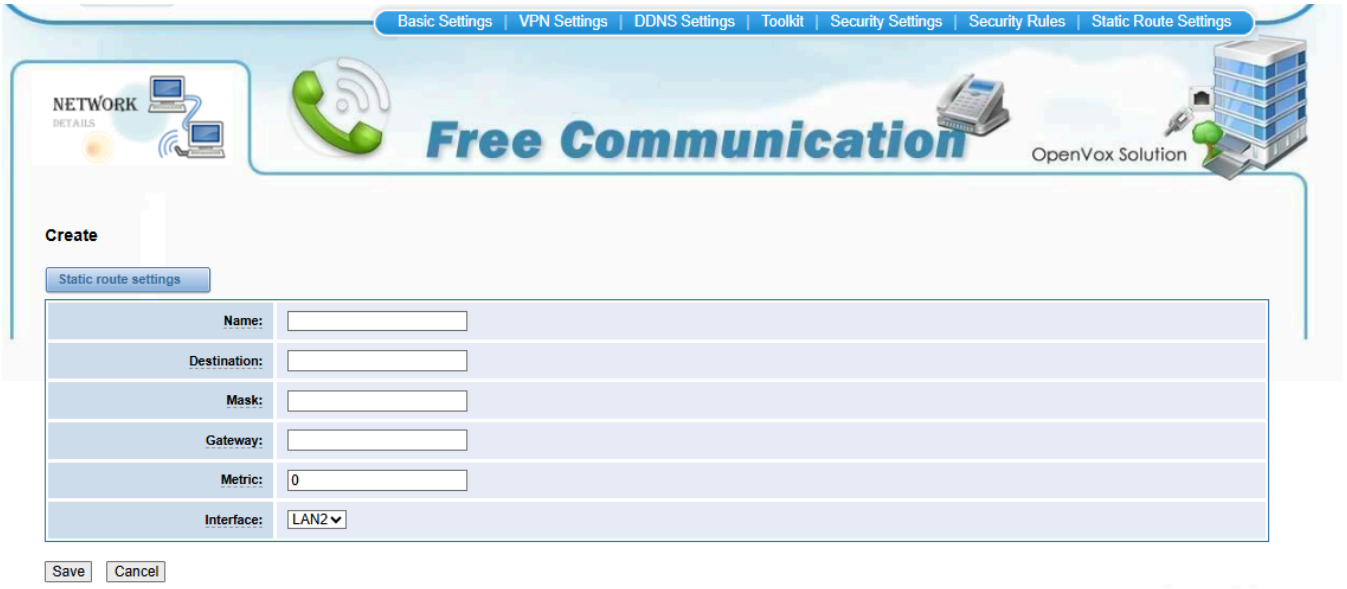


Parameter Name	Description	Recommended Configuration
Rule Name	Set the firewall rule name.	Name it according to service purpose.
Protocol	Set the network protocol matched by the rule.	Select according to the actual service.
Port	Set the port range matched by the rule.	For a single-port service, enter the same start and end ports.
IP / MASK	Set the address range matched by the rule.	Use precise source ranges according to the actual source.
Action	Set the processing method after the rule is matched.	For legitimate services, set it to ACCEPT.

6.7 Static Routing Settings

This page is mainly used to configure static routes so the device can access other network segments or specified network exits. In multi-subnet networking scenarios, fill in related parameters correctly according to the site network topology.

Click `Add`. The interface is shown below.



Parameter Name	Description	Recommended Configuration
Name	Set the static route name.	Name it according to purpose.
Destination	Set the target subnet address.	Enter the target network address.
Mask	Set the target subnet mask.	Keep it consistent with the target subnet.
Gateway	Set the next-hop gateway.	Enter a reachable upstream router address.
Hop Count	Set route priority.	Keep the default setting in most cases.
Interface	Set the route outbound interface.	Select the interface that can reach the gateway.

7. Advanced Options

Go to the `Advanced Options` menu. In Advanced Options, you can configure the following sections:

- Asterisk Application Interface
- Asterisk Command Line Interface
- Asterisk File Editor
- Cloud Management

- TR069
- SNMP
- Auto Provisioning

7.1 Asterisk Application Interface

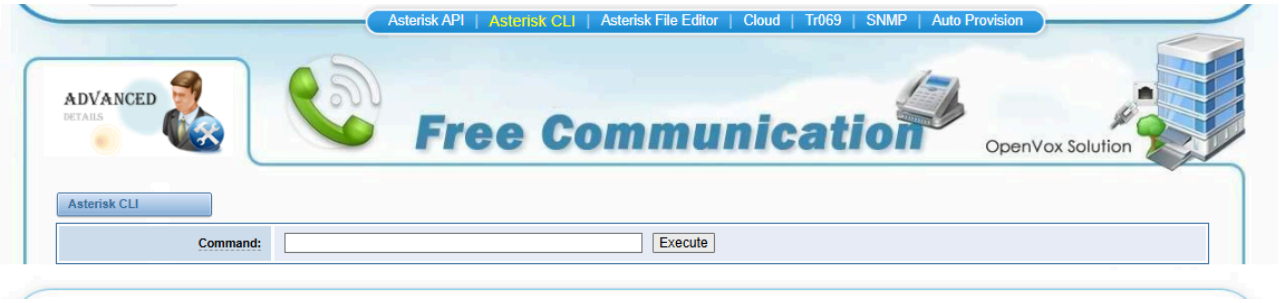
This page is mainly used to configure Asterisk AMI interface parameters so third-party platforms can manage and exchange status with the device. Before enabling it, confirm the access source, authentication information, and permission scope.

Option	Definition
Port	Network port number.
Manager Name	The manager name cannot contain spaces.
Manager Password	Manager password. Available characters: "-_+.<>&0-9a-zA-Z". Length: 4-32 characters.

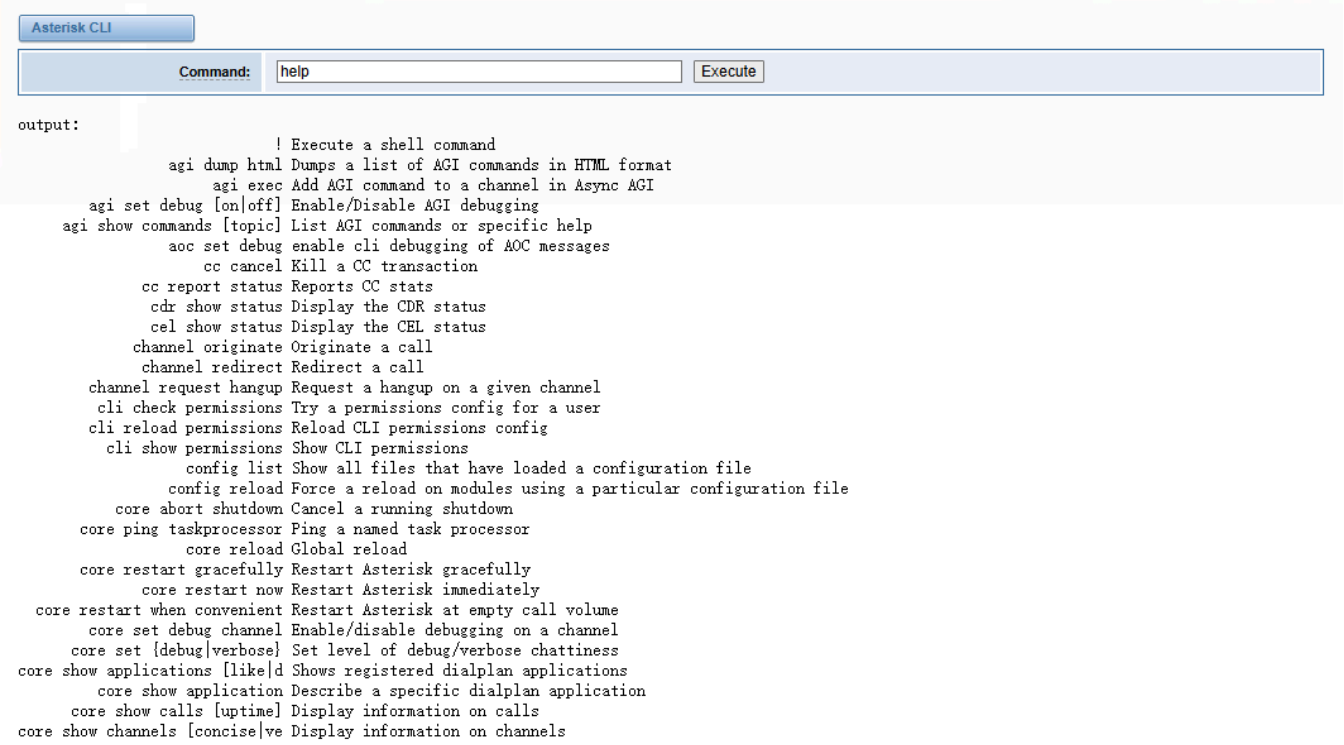
Option	Definition
Deny	If you want to deny access from certain networks or hosts, use & as the separator. For example: 0.0.0.0/0.0.0.0 or 192.168.1.0/255.255.255.0&10.0.0.0/255.0.0.0.
Permit	If you want to allow access from certain networks or hosts, use & as the separator. For example: 0.0.0.0/0.0.0.0 or 192.168.1.0/255.255.255.0&10.0.0.0/255.0.0.0.
System	Basic system information and common system management commands, such as shutdown, reboot, and reload.
Call	Channel information and settings of active channels.
Log	Log information. Read-only. Defined but not used.
Verbose	Debug information. Read-only. Defined but not used.
Command	CLI commands allowed to run. Read-only.
Agent	Queue and agent information and the ability to add queue members to queues.
User	Allows sending and receiving user events.
Config	Ability to read and write configuration files.
DTMF	Receives DTMF. Read-only.
Reporting	Ability to obtain system information.
Dialplan	Receives NewExten and VarSet events. Read-only.
Originate	Allows originating new calls. Read-only.
Select All	Select or clear all selections.

7.2 Asterisk Command Line Interface

This page is mainly used to execute Asterisk command line instructions. It can be used to view system status, debug call flows, and assist fault analysis. It is recommended for maintenance personnel with related experience.



Option	Definition
Command	Type an Asterisk console command to view or debug the gateway. For example, type "help" or "?" to view all help information.



7.3 File Editor

This page is mainly used to edit Asterisk configuration files online for advanced service customization. Before modification, back up the original files and reload services as needed after the modification is complete.

7.4 Cloud Management

This page is mainly used to configure connection parameters between the device and the cloud management platform to support centralized remote management. Before enabling it, confirm that the device has available external network access.

Parameter Name	Description	Recommended Configuration
Interface	Select the network interface used to connect to the cloud platform.	Select an interface with Internet access.
Enable Cloud Management Service	Set whether to enable cloud management.	Enable when remote management is required.
Select Server	Select the cloud platform server region.	Select according to deployment region.
Account	Enter the cloud management platform account.	Enter the actual account.
Password	Enter the cloud management platform password.	Enter the actual password.

7.5 TR069

This page is used to configure parameters required for the device to access a TR-069 remote management platform, including ACS server address, authentication information, periodic notification, and callback configuration. After it is enabled and correctly configured, the device can establish a connection with the remote management platform through TR-069 to implement remote configuration delivery, status collection, and unified operation and maintenance management. During deployment, accurately enter the server address, username, password, and notification interval according to parameters provided by the platform, and check whether the connection status is normal after saving.

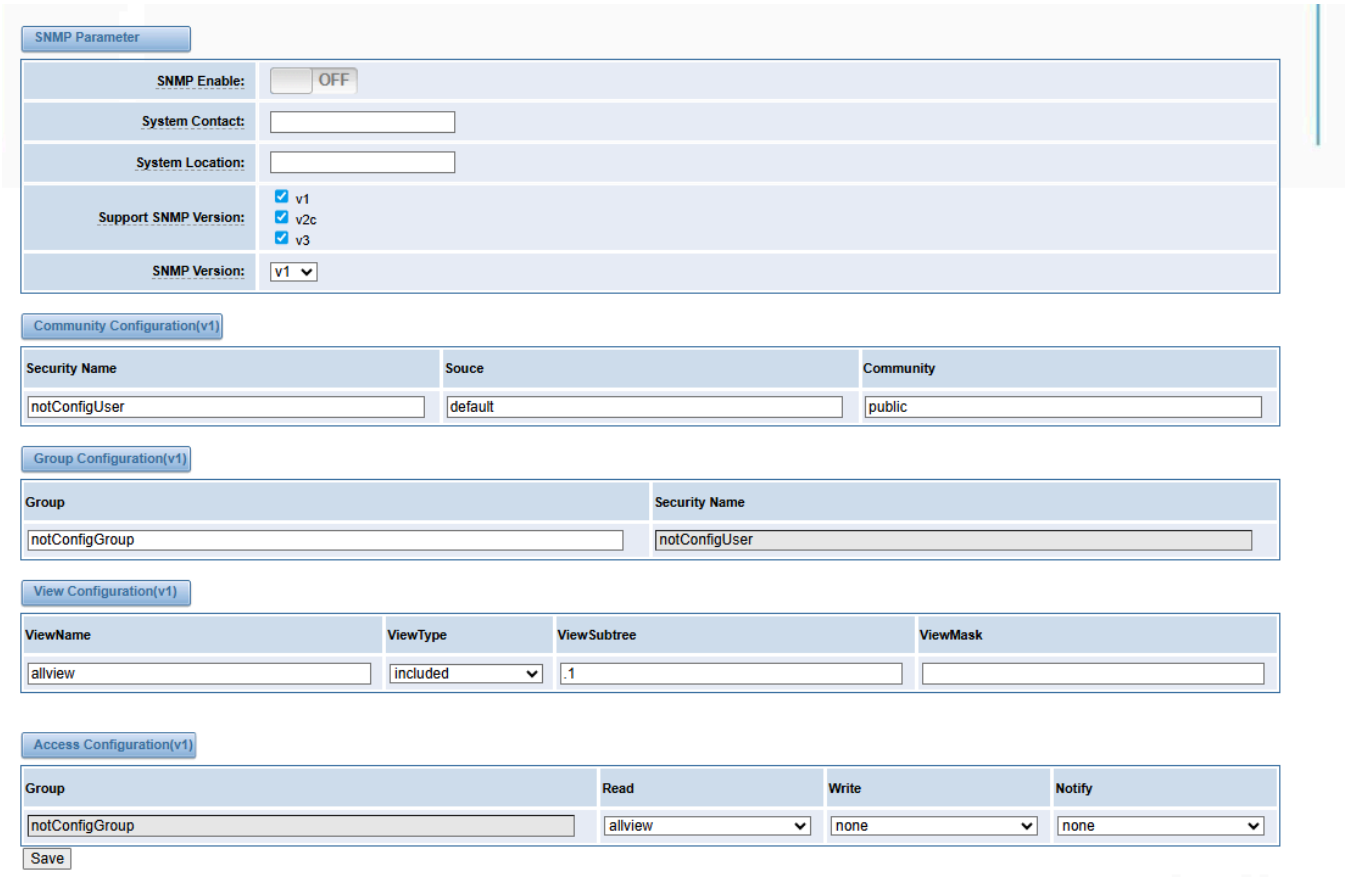
Parameter Name	Description	Recommended Configuration
TR069	Set whether to enable TR-069 management.	Enable when remote management is required.
Server URL	Set the ACS server address.	Enter the address provided by the platform.
Username	Set the ACS login username.	Enter the platform account.
Password	Set the ACS login password.	Enter the platform password.
Service Provider Identifier Code	Set the service provider or platform identifier.	Enter according to project requirements.
Module Name	Set the device module name.	Keep the default setting in most cases.
Periodic Notification Switch	Set whether to periodically report status.	Enable when periodic reporting is required.
Periodic Notification Interval	Set the reporting period.	Enter according to platform requirements.
Callback Address	Set the platform callback address.	Enter according to platform requirements.
Callback Authentication Account	Set the callback authentication account.	Enter according to platform requirements.

Parameter Name	Description	Recommended Configuration
Callback Authentication Password	Set the callback authentication password.	Enter according to platform requirements.
Connection Status	Display the current connection result.	If it fails, check configuration and network.

7.6 SNMP

This page is mainly used to configure SNMP network management so the platform can monitor and collect information from the device. Restrict access sources and avoid using the default community string.

This page is used to configure the SNMP management function of the device, including basic parameters, communities, groups, views, and access permissions. With correct SNMP configuration, the network management platform can monitor device operation status, collect information, and manage devices centrally. During deployment, select a suitable SNMP version according to network management platform requirements, and restrict community and access source ranges to improve management security.

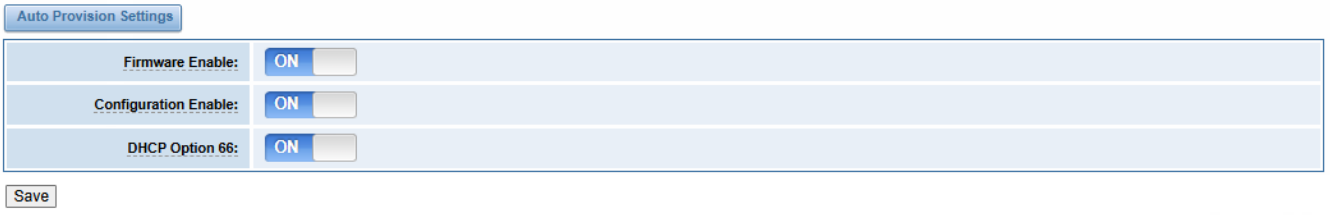


Parameter Name	Description	Recommended Configuration
Enable SNMP	Set whether to enable SNMP.	Enable when connecting to a network management platform.
System Contact	Set the maintenance contact.	Enter the actual contact.

Parameter Name	Description	Recommended Configuration
Address	Set the device deployment location.	Enter site information.
SNMP Version	Set the SNMP version to use.	Configure according to network management platform requirements.
Community	Set the SNMP access string.	Do not use the default public string.
IP Address Range	Set the allowed access source range.	Restrict it to trusted addresses.
Group	Set the permission group.	Configure according to management purpose.
View Name	Set the access view name.	Name it according to purpose.
Read	Set the read permission view.	Read-only is usually sufficient.
Write	Set the write permission view.	Keep none when write access is not required.
Notify	Set the notification permission view.	Configure only when Trap is required.

7.7 Auto Provisioning

This page is mainly used to configure the device capability to automatically obtain firmware and configuration files. It applies to centralized deployment and unified upgrade scenarios. Before official enablement, confirm that the server address and delivery policy are correct.



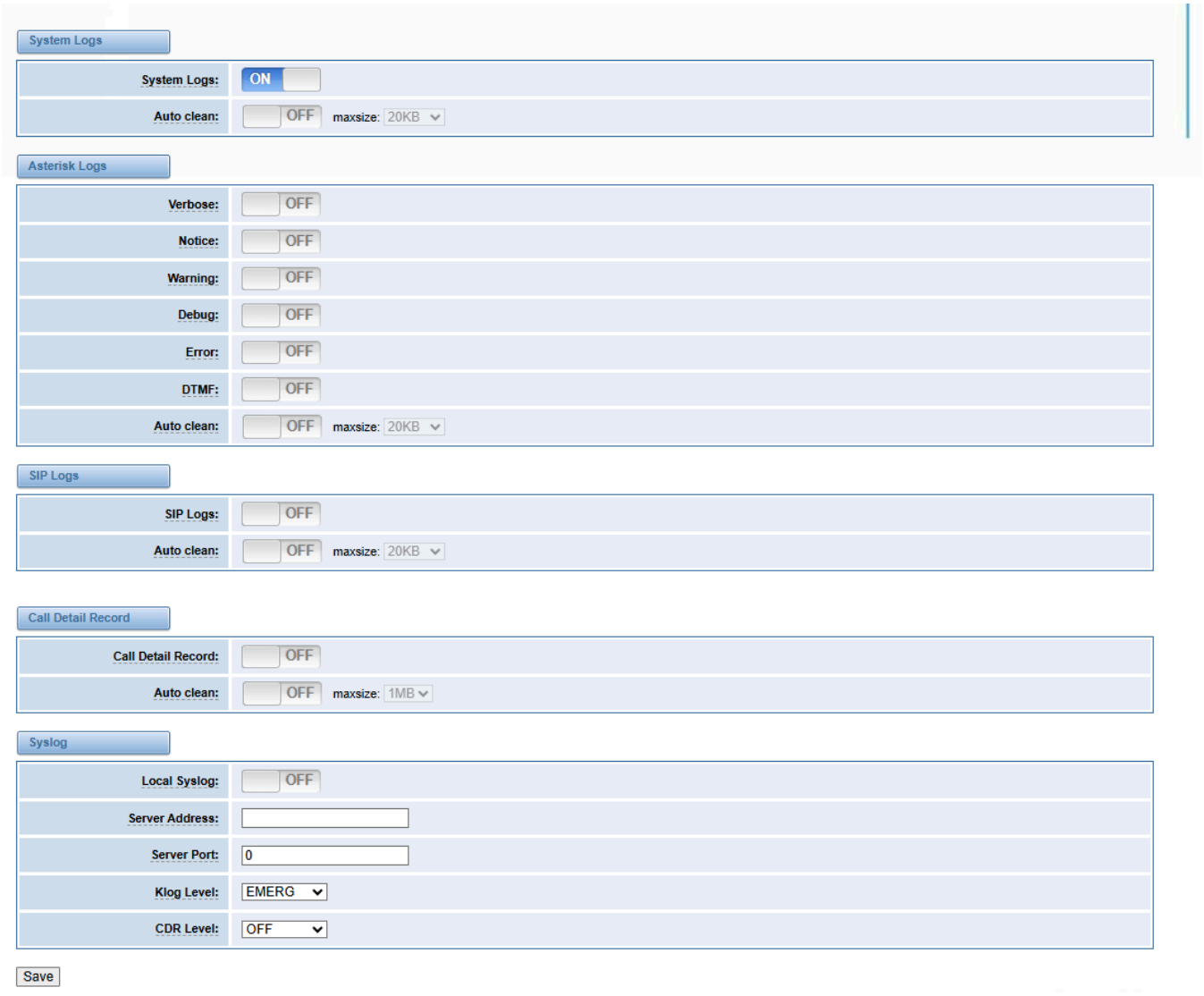
Parameter Name	Description	Recommended Configuration
Firmware Switch	Set whether to automatically obtain or upgrade firmware.	Enable for batch upgrade.
Configuration File Switch	Set whether to automatically download configuration files.	Enable for centralized deployment.
DHCP Option 66	Set whether to obtain the configuration server address through DHCP.	Enable when automatic delivery through DHCP is used.

8. Logs

On the Log Settings page, enable the related log on the corresponding log page. For example, enable SIP Log as shown below, and then go to the SIP page to view SIP logs. Otherwise, no content is output in the SIP log. The same applies to other log pages.

8.1 Log Settings

This page is mainly used to enable and manage various log outputs, including system logs, Asterisk logs, SIP logs, and call statistics. Before troubleshooting, confirm that the corresponding log has been enabled.



System Log Output

Table 9-1-1 Log Definitions

Option	Definition
Auto Clear (System Log)	On: When the log file reaches the configured maximum size, the system deletes half of the file. New logs are written in. Off: Logs are retained and continue to grow. Default: On. Default size: 1 MB.
Verbose	Verbose output information from the Asterisk console.
Notice	Notice information from the Asterisk console.
Warning	Warning information from the Asterisk console.
Debug	Debug information from the Asterisk console.
Error	Error information from the Asterisk console.
DTMF	DTMF information from the Asterisk console.
Auto Clear (Asterisk Log)	On: When the log file reaches the configured maximum size, the system deletes half of the file. New logs are written in. Off: Logs are retained and continue to grow. Default: On. Default size: 2 MB.
SIP Log	Enable or disable SIP logs.
Auto Clear (SIP Log)	On: When the log file reaches the configured maximum size, the system deletes half of the file. New logs are written in. Off: Logs are retained and continue to grow. Default: On. Default size: 2 MB.
IAX2 Log	Enable or disable IAX2 logs.
Auto Clear (IAX2 Log)	On: When the log file reaches the configured maximum size, the system deletes half of the file. New logs are written in. Off: Logs are retained and continue to grow. Default: On. Default size: 2 MB.
MFC/R2 Log	Enable or disable MFC/R2 logs.

Option	Definition
Auto Clear (MFC/R2 Log)	On: When the log file reaches the configured maximum size, the system deletes half of the file. New logs are written in. Off: Logs are retained and continue to grow. Default: On. Default size: 2 MB.
PRI Log	Enable PRI logs. One or more ports can be selected. If All is selected, the PRI page displays logs for all ports.
Auto Clear (PRI Log)	On: When the log file reaches the configured maximum size, the system deletes half of the file. New logs are written in. Off: Logs are retained and continue to grow. Default size should be set on the Log Settings page. Enable the related log on the corresponding log page. For example, enable SIP Log as shown below, and then go to the SIP page to view SIP logs. Otherwise, SIP logs are unavailable. The same applies to other log pages.
SS7 Log	Enable or disable SS7 logs.
Auto Clear (SS7 Log)	On: When the log file reaches the configured maximum size, the system deletes half of the file. New logs are written in. Off: Logs are retained and continue to grow. Default: On. Default size: 2 MB.
Call Statistics	Enable or disable call statistics.
System Notifications	Receive pushed system upgrade notifications and auto provisioning upgrade notifications.

8.2 System Log

This page is mainly used to view device system-level event records, including power on/off, power failure, and upgrade information. It can help locate system exceptions or maintenance operation records.

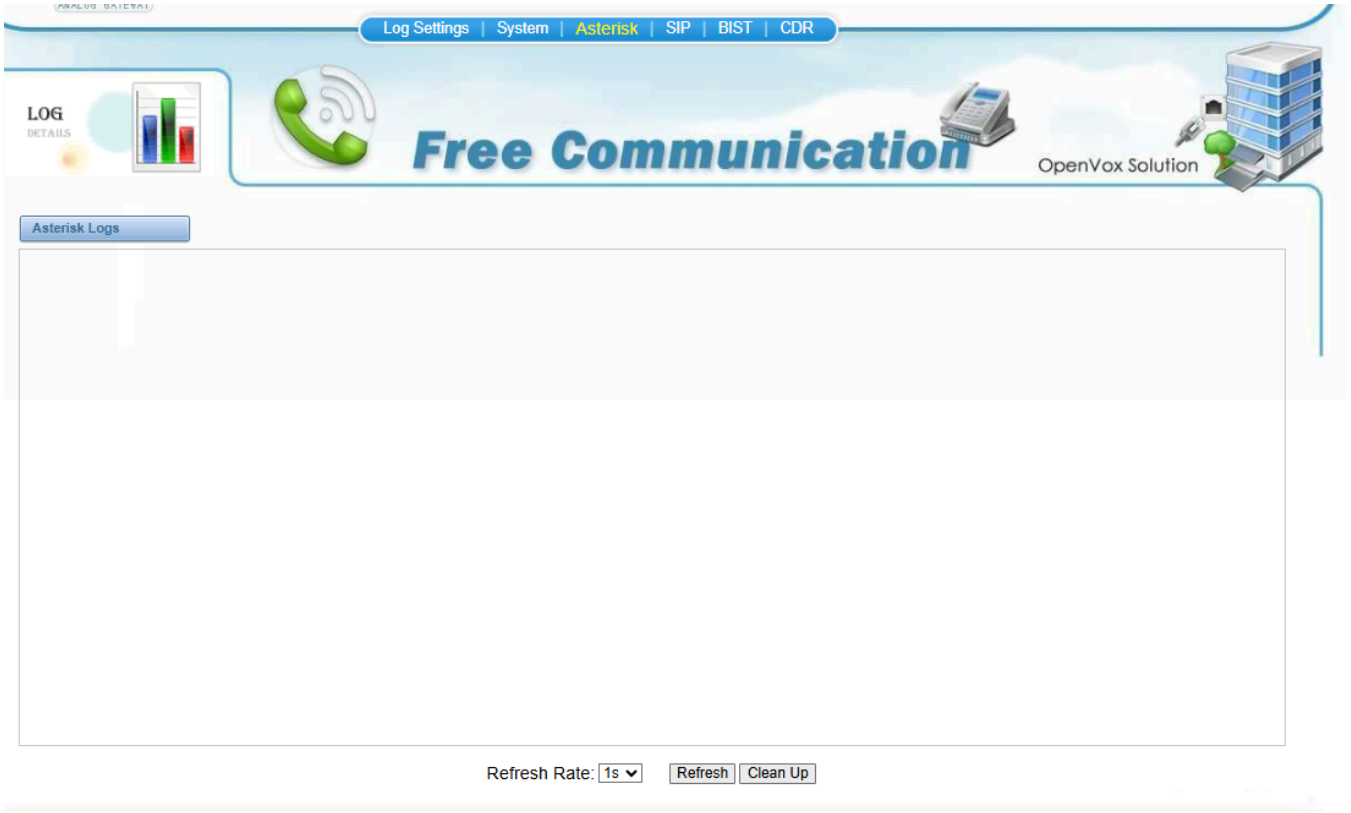
System logs record each power on/off, power failure, and firmware upgrade event.

Figure 9-2-1 System Log

8.3 Asterisk Log

This page is mainly used to view Asterisk-related log information, helping analyze call processing and system operation status. Use it together with SIP logs and packet capture information to determine causes.

On the System, Asterisk, SIP, IAX2, SS7, and MFC/R2 pages, there are functions for displaying logs by port, periodic update, and log download.



8.4 Call Statistics

This page is mainly used to view call statistics of the device, including answered calls, failures, no-answer calls, and accumulated duration. This function is suitable for operation analysis and service quality evaluation.

In call statistics, you can see Answered, Blocked, Call Busy, Call Failed, No Answer, Other, Current Calls, Accumulated Calls, Total Call Duration, and ASR. ASR stands for Answer Seizure Ratio. Total Call Duration is the total call time of all calls on the gateway. Call statistics data is saved before power-off and restored after power-on. It can refresh automatically. You can also manually clear statistics.

Note: If call record statistics are required, remember to enable Call Statistics in Log Settings.