Redstone Systems, Inc.

REX Series IP Telephony System

REX8000

Administrator's Manual

Document Version: 2024-12

Release Date: 2024-12-16

Amendment Records

Document Rev. 02(2024-12-16)

Updated based on GA version.

Document Rev. 01(2019-12-13)

Full Text.

Copyright © 2025 Redstone Systems, Inc. All Rights Reserved.

All or part of this document may not be excerpted, reproduced and transmitted in any form or by any means without prior written permission from the company.

Manual Description

This manual applies to the REX8000.

Web site: https://www.redstonesystems.com/

Tel：4259006090

Mail：globalmarketing@redstonesystems.com

Contents

Amendment Records 2
Manual Description 3
Contents 4
Contents of Figures 6
Contents of Tables 8
1 Overview 10
1.1 Overview 10
1.2 Product Characteristics 11
1.3 Product Specification 12
1.4 Hardware and Software Module Composition 13
2 Configuring Basic Functions 16
2.1 Logging in to the Web 16
2.2 Configuration Wizard 17
2.2.1 Step 1: Hardware Confirmation 17
2.2.2 Step 2: Network Configuration 18
2.2.3 Step 3: IP Extensions 18
2.2.4 Step 4: SIP Outbound 19
2.2.5 Step 5: Outbound Calling Rules 19
2.2.6 Step 6: Configuration Completed 20
3 Configure Personalization Features 21
3.1 Condition Monitoring 21
3.1.1 Device Status 21
3.1.2 Extension Status 25
3.1.3 Outsider Status 26
3.1.4 System Status 28
3.2 Basic Settings 32
3.2.1 Network Setup 32
3.2.2 Outgoing Rule 37
3.2.3 Central Exchange 39
3.2.4 Multi-level IVR 44
3.2.5 Voice management 48
3.3 Extension Setup 51
3.3.1 IP Extension 51
3.3.2 Department 62
3.3.3 Call Number Binding Table 64
3.4 External line setup 65

3.4.1 SIP Outbound 65
3.4.2 Direct relay group 74
3.4.3 DOD Number 75
3.5 Application Service 76
3.5.1 Media, Esp. News Media 76
3.5.2 API 77
3.5.3 Sound Recordings 81
3.5.4 Call limit 82
3.5.5 Secretary 83
3.5.6 Duty Roster 84
3.6 Advanced Settings 90
3.6.1 Systems 90
3.6.2 Certificates 92
3.6.3 Function Code 92
3.6.4 Dial Detection and Bitmap 93
3.6.5 SIP Compatibility 96
3.6.6 Routing Table 98
3.6.7 Network Management 106
3.7 Security Center 109
3.7.1 Safety Configuration 109
3.7.2 Access To A White List 112
3.7.3 Brute Force Account Cracking Prevention 114
3.7.4 Static Defense 115
3.7.5 Encrypted 117
3.8 System Maintenance 119
3.8.1 Board Management 119
3.8.2 System expansion 120
3.8.3 Alarm Management 121
3.8.4 Configuration Management 124
3.8.5 Version Management 125
3.8.6 Log Management 126
3.8.7 System Tools 128
3.9 Rights Management 136
3.9.1 User List 136
3.9.2 Operating Log 137
3.9.3 Modify A Password 138
3.10 Network Setup 139
4 Common Problems 143
4.1 IP Outbound Registration Issues 143

Contents of Figures

Figure1-1 Front panel 13
Figure1-2 Rear panel 14
Figure2-1 login screen 16
Figure3-1 switching mode 33
Figure3-2 802.1X Configuration Interface 37
Figure3-3 Auto Attendant Configuration Screen 39
Figure3-4 IVR1 Configuration Interface 47
Figure3-5 Background Music Configuration Interface 50
Figure3-6 Number Filtering Configuration Interface 62
Figure3-7 Department Configuration Screen 63
Figure3-8 Incoming Call Binding Table Screen 64
Figure3-9 SIP Outbound New Interface 65
Figure3-10 SIP Outbound Configuration Interface 68
Figure3-11 SIP Outbound Registration Options Screen 71
Figure3-12 Linear (DID/DOD) Configuration Interface 76
Figure3-13 Media Configuration Interface 76
Figure3-14 API Configuration Interface 78
Figure3-15 Remote Recording Configuration Interface 81
Figure3-16 Extension Recording Configuration Interface 81
Figure3-17 Call barring configuration screen 82
Figure3-18 Attribution area code configuration screen 90
Figure3-19 DTMF interface 91
Figure3-20 Function Code Configuration Screen 92
Figure3-21 Dialing Rule Configuration Screen 94
Figure3-22 SIP Compatibility Interface 96
Figure3-23 Routing Table Configuration Interface 99
Figure3-24 Routing Table Configuration Interface - Call Length Restriction 101
Figure3-25 TR069 Configuration Interface 107
Figure3-26 SNMP Configuration Interface 108
Figure3-27 Web Management Configuration Interface 110
Figure3-28 Voice Security Configuration Interface 111
Figure3-29 Whitelist Configuration Screen 113
Figure3-30 Brute force account (login retry lockout) configuration screen 114
Figure3-31 Anti-breakdown account (lock list) screen 115

Figure3-32 Static Defense Configuration Interface 116
Figure3-33 Cryptographic Interface 117
Figure3-34 Software Upgrade Screen 125
Figure3-35 Log Download Screen 126
Figure3-36 System Time Configuration Screen 128
Figure3-37 Voice Pack Configuration Interface 129
Figure3-38 Ping Diagnostic Interface 132
Figure3-39 network interface 140
Figure3-40 Network Configuration Interface 140
Figure3-41 Add Site Screen 141

Contents of Tables

Table1.1 Performance specifications 12
Table1.2 Hardware Specifications 12
Table1.3 Indicator light meaning table 14
Table1.4 Interface Description 15
Table2.1 Login Interface Parameters 17
Table3.1 Description of Device Status 24
Table3.2 Description of Equipment Name 32
Table3.3 Parameter description 33
Table3.4 IMS Dedicated Access Mode Parameter Description 35
Table3.5 802.1X Interface Parameter Description 37
Table3.6 Outbound call rule parameter description 38
Table3.7 Automated Operator Parameters 40
Table3.8 Factory Default Voice File 40
Table3.9 Microphone Recording Welcome Note 41
Table3.10 Operator Configuration Screen 43
Table3.11 Operator Parameters 43
Table3.12 Multi-level IVR 45
Table3.13 Multi-level IVR 47
Table3.14 IP Extension Configuration Parameter Description 52
Table3.15 IP Extension Configuration Parameter Description 58
Table3.16 IP Extension Parameter Description 61
Table3.17 Parameter Description of Number Filtering Interface 62
Table3.18 Parameter Description of Sectoral 63
Table3.19 Parameter Description of Caller Binding Number Form 64
Table3.20 Description of SIP outbound registration parameters 66
Table3.21 SIP Outbound Interface Parameter Description 68
Table3.22 Parameter Description of SIP Outbound Registration Options 71
Table3.23 Description of media parameters 77
Table3.24 API Interface Parameter Description 78
Table3.25 Extension API Switch Parameter Description 79
Table3.26 Outside API switch Parameter Description 80
Table3.27 Outside API switch Parameter Description 83
Table3.28 Duty roster Parameter Description 85
Table3.29 Duty roster Parameter Description 87

Table3.30 Duty roster Examples 88
Table3.31 Explanation of attributed area code parameters 91
Table3.32 DTMF Parameter Description 91
Table3.33 Function code Parameter Description 93
Table3.34 Explanation of the rules of the common numbered digit map 94
Table3.35 SIP Compatibility Parameter Description 96
Table3.36 Interface Configuration Rules Description 100
Table3.37 Interface Configuration Rules 102
Table3.38 Interface Configuration Rules 105
Table3.39 TR069 Parameter Description 107
Table3.40 SNMP Parameter Description 108
Table3.41 SSH Configuration Interface 109
Table3.42 Responding to Ping Requests Parameter Description 110
Table3.43 Web Management Interface Parameter Description 111
Table3.44 Description of voice security interface parameters 111
Table3.45 Description of whitelisting parameters 113
Table3.46 Anti-brute-force account break-in (login retry lockout) parameters 114
Table3.47 Anti-brute-force account (lockout list) display information 115
Table3.48 Static defense parameters 116
Table3.49 Description of encryption parameters 117
Table3.50 Description of Board Management 119
Table3.51 Classification of alarm messages 123
Table3.52 Log Download 126
Table3.53 Log Backup 127
Table3.54 Log Backup 127
Table3.55 Description of system time parameters 128
Table3.56 System voice prompt file 129
Table3.57 Authorization Management Parameters 135
Table3.58 Security Policy Parameters 140
Table3.59 Site Add Interface Parameters 141
Table4.1 Solution to SIP Outbound Registration Problems 143

1 Overview

1.1 Overview

REX8000 fusion communication platform is a new generation of IP voice core switching equipment launched by RedStone Systems. Fulfill the single point of more than 1,000 extensions, distribution network up to tens of thousands of extensions of government agencies and groups of enterprises of large-capacity telephone deployment needs. REX8000 provide voice calls, video calls, high-speed faxes, teleconferencing, telephone recording, mobile extensions, and other integrated converged communication solutions.

REX8000 has powerful call processing capability, supporting 8000 user extension and 800 concurrent calls. It also excels in stability, reliability, security, scalability and configuration flexibility.

REX8000 supports direct connection with operator's voice service platform through SIP trunks (including IMS), connection with operators or other voice networks through digital trunks， analog trunks, and access to terminals such as analog phones, fax machines, POS machines, IP phones, video phones, and PC/cell phones/PAD softphones, etc. It is suitable for single-point deployment in large and medium-sized enterprises, it meet the needs of multi-point telephone networks of large group enterprises and government agencies through Internet/VPN. VPN to meet the needs of large groups of enterprises, government agencies and other multi-point telephone network.

 Copyright © RedStone Systems, Inc

1.2 Product Characteristics

Rich business and interface capabilities

- Support voice, video, fax, conference, recording and other IP voice services
- Supports SIP trunks (including IMS), digital trunks ① and analog trunks ②.
- Supporting the provision of recording management system, teleconferencing system, unified equipment management system, network server system, hotel management system docking middleware, helpdesk system and other application services
- Support docking third-party applications and API secondary development

High performance, high stability

- Distributed architecture design with clustered provisioning of media resource cards
- Parallel processing of call operations for faster response times
- Automatic load balancing

Multiple redundancy and security mechanisms

- Dual chassis hot standby, primary and secondary switchover time <5 seconds
- 1+1 redundancy for power supply/network port/master control card, N+1 redundancy for media resource card
- Encryption of signaling, media and data transmission
- Support mechanisms such as access whitelisting, extranet user authorization, long-distance call restriction, etc.

Flexible deployment, simple operation and maintenance

 Copyright © Redstone Systems, Inc

- Support single-point centralized deployment, multi-point distributed networking
- Supports unified management of equipment, efficient operation and maintenance
- Supports graphical configuration interface
- Support Phone/Email/WeChat Failure alarms

External RedStone digital trunking gateway (stand-alone support 1/2/4 30B+D interfaces)

External RedStone analog gateway (stand-alone support for 2-96 FXO ports)

Use in conjunction with the RedStone equipment unified management system

1.3 Product Specification

Table1.1 Performance specifications

Item	Description
IP extension license	8000 extensions
IP trunk license	8,000 trunks
Number of concurrent calls	800 concurrent (with recording)
Call handling capacity	37,000 calls completed per hour during busy periods (BHCC)
H x W x D	Single chassis: 44 x 442 x 420mm (1U) Dual chassis: 88 x 442 x 420mm (2U)

Table1.2 Hardware Specifications

Item	Description
Single-Unit Frame	Main control card × 1, fan module × 1, power supply module × 1 or 2, free slots × 4
Media Resource Card	Single card supports 1000 IP extensions, 125 concurrent calls (with recording), supports hot-swapping; single frame is fully equipped with 4 media resource cards
Network Port	RJ45, 2 x 10/100/1000 Base-T, Adaptive
CON Port	RJ45

 Copyright © Redstone Systems, Inc

Item	Description
Internal Storage	64GB
H X W X D	Single chassis: 44 x 442 x 420mm (1U) Dual stacking: 88 x 442 x 420mm (2U)
Net Weight	7.5kg (single chassis full)
Single/Dual AC Power Supply	100 to 240 volts, 50/60 Hz, 1 ampere
Installation	19-inch rackmount
Working Environment	Temperature: 0℃ ~ 40℃; Relative humidity: 10% ~ 90% (non-condensing)
Storage Environment	Temperature: -40℃ ~ 70℃; Relative humidity: 5% ~ 90% (non-condensing)
Height Above Sea Level	Below 2000 meters
Climatic Conditions	Recommended non-tropical

1.4 Hardware and Software Module Composition

Figure1-1 Front panel

Single chassis



Dual chassis



 Copyright © Redstone Systems, Inc

Figure1-2 Rear panel

Single chassis



Dual chassis



Table1.3 Indicator light meaning table

Indicator light	Flashing light status	Particular
PWR (Green)	Green and bright	Power on.
	Off	Power not connected
STU (Red, Green)	Red and shiny	During reboot or upgrade In addition, the STU and ALM of all boards are flashing red to indicate that the chassis numbers of the two chassis are in conflict when dual stacked
	Green and shiny	Normalcy
	Green and bright	Standby chassis normal when dual stacked
	Red, long-lasting light	Fault: The board does not work, or the board is not recognized, power down, or the network cable is disconnected. In addition, the STU and ALM of all boards are red and long lit to indicate that the chassis number is not recognized (normal chassis numbers can only be 1 or 2)
	Alternate flashing red and green	SIP outbound registration failure In addition, alternating red and green blinking of the STU and ALM on all boards indicates IP address conflicts
	Off	deactivate
RUN	Green and bright	The power supply is normal.
ALM (Red, Green)	Off	trouble-free
	Red, long-lasting light	Fault: The board does not work, or the board is not recognized, power down, or the network cable is disconnected. The STU and ALM of all boards are red and long lit to indicate that the chassis number is not recognized (normal chassis numbers can only be 1 or 2)
Network Port	Long green light on the right side	1000Mbps

 Copyright © Redstone Systems, Inc

Indicator light	Flashing light status	Particular
Lights (Left and Right Sides)	Right side off	10/100Mbps
	Long green light on the left side	Physical link established, but no network traffice flow
	Shiny green on the left side	Physical links have been established and there is a network traffice Flow
	Left side off	No physical link established

Table1.4 Interface Description

Connector	Instructions
CONSOLE	Configuration port for local management and debugging.
ETH1/ETH2	Gigabit Ethernet port, working in switching mode by default. Default IP address: 192.168.2.240. The IP address can be modified in "Basic Settings > Network Configuration".
AUX1/AUX2	Used for dual chasis interconnection when dual chasis are stacked.
	AC power input connector for 100V to 240V alternating current (AC) voltage.
	Grounding post.
CID	Chassis number. If it is a single chasis, set it to 1. For dual chasis, one is set to 1 and the other to 2.

 Copyright © Redstone Systems, Inc

2 Configuring Basic Functions

2.1 Logging in to the Web

Step1. Connect the computer and the device's ETH1/ETH2 interface with a network cable (or make sure the computer and the device are on the same LAN).

Step2. Set the IP address of the computer to be in the same network segment as the IP address of the device (default 192.168.2.240).

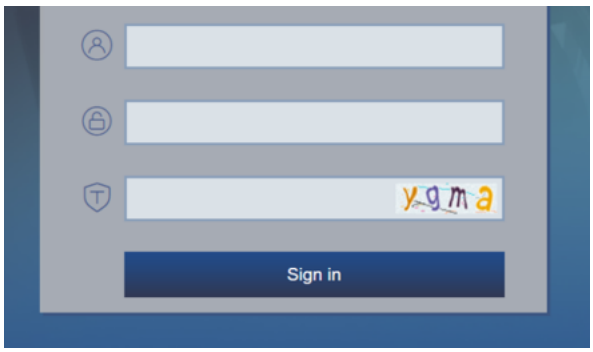
Step3. Enter the IP address of the device in the address bar of your computer's browser to open the login screen.

Step4. On the login screen, enter your identity to select your language and enter your password to log in to the device. The default administrator account is admin and the password is admin.

Note

- Accessing the device with HTTP is automatically switched to using HTTPS. Since the certificate provided by the factory is used, for example, in IE browser, there is a prompt "There is a problem with the security certificate of this website", and the login page can be accessed after clicking "Continue to browse this website".
- Directly close the browser can not automatically exit the login, you need to click in the upper right corner of the web interface to exit.

Figure2-1 login screen



 Copyright © RedStone Systems, Inc

Table2.1 Login Interface Parameters

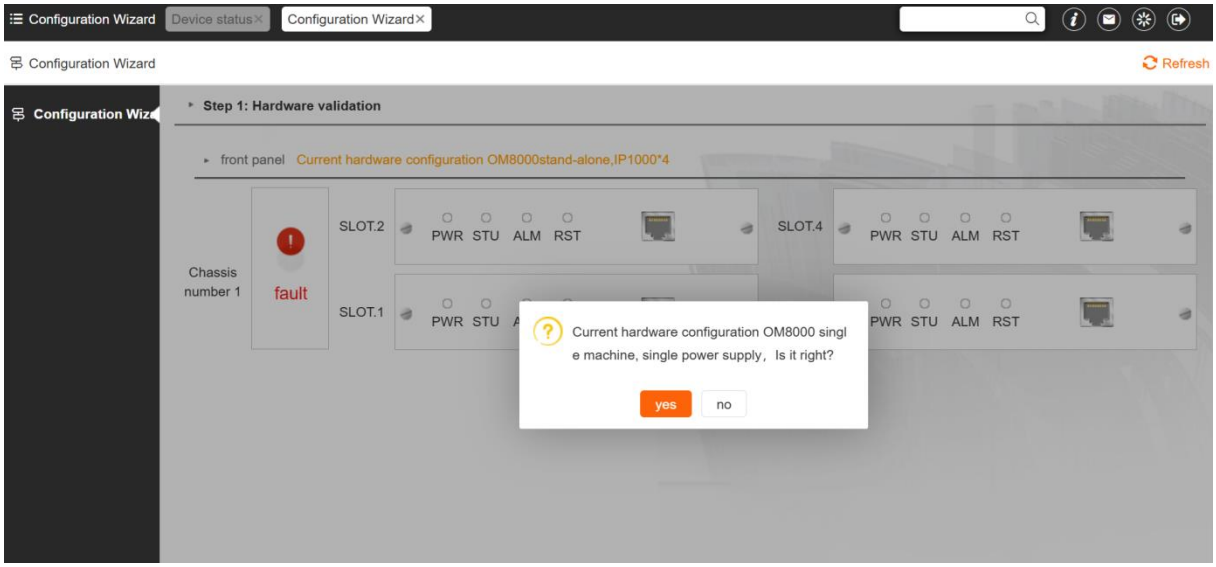
sports event	Description
Chinese/EN	Select the interface language as Chinese or English.
Username	The device provides two levels of administrative privileges: ● admin: the default super administrator of the system. ● Ordinary Administrator: account is created by admin after logging in to the device, and account permissions are defined by admin when it is created. The system can have multiple general administrator accounts.
Password	The password for the super administrator admin defaults to admin. The general administrator password is set when the account is created by admin.
CAPTCHA, A Type Of Challenge-Response Test (Computing)	Consists of 4 digits and letters. If the CAPTCHA image is not clear, you can click on the image to change it.

2.2 Configuration Wizard

When configuring the device for the first time, the Configuration Wizard is recommended.

2.2.1 Step 1: Hardware Confirmation

The page will prompt the current hardware composition, please confirm according to the actual situation, if not correct, please check the line connection.

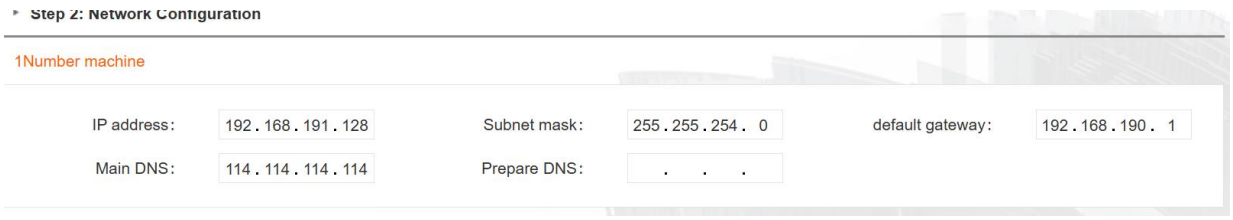


2.2.2 Step 2: Network Configuration

Used to configure the device IP address, subnet mask, gateway address, and DNS address.

Single chassis

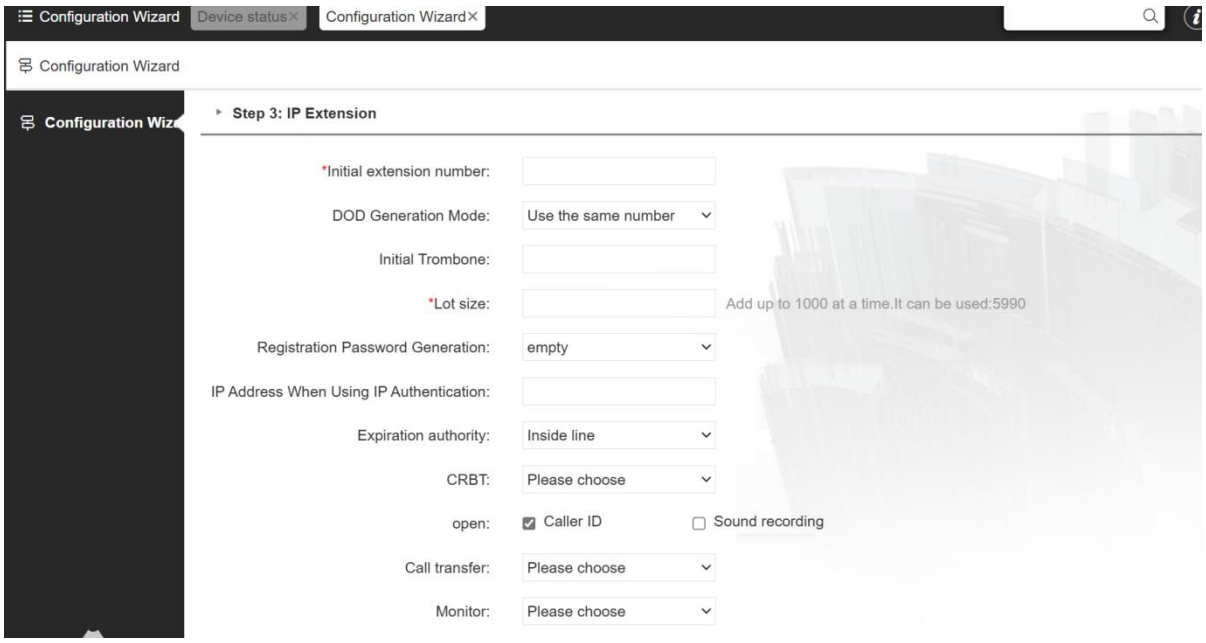
In the single chassis case, there is only one IP address in switching mode.



Dual chassis

In the dual chassis case, chassis 1 and 2 each have an address for dual interconnect or for logging into a chassis individually. Another whole external IP address is the address that the dual device displays externally as a whole.

2.2.3 Step 3: IP Extensions



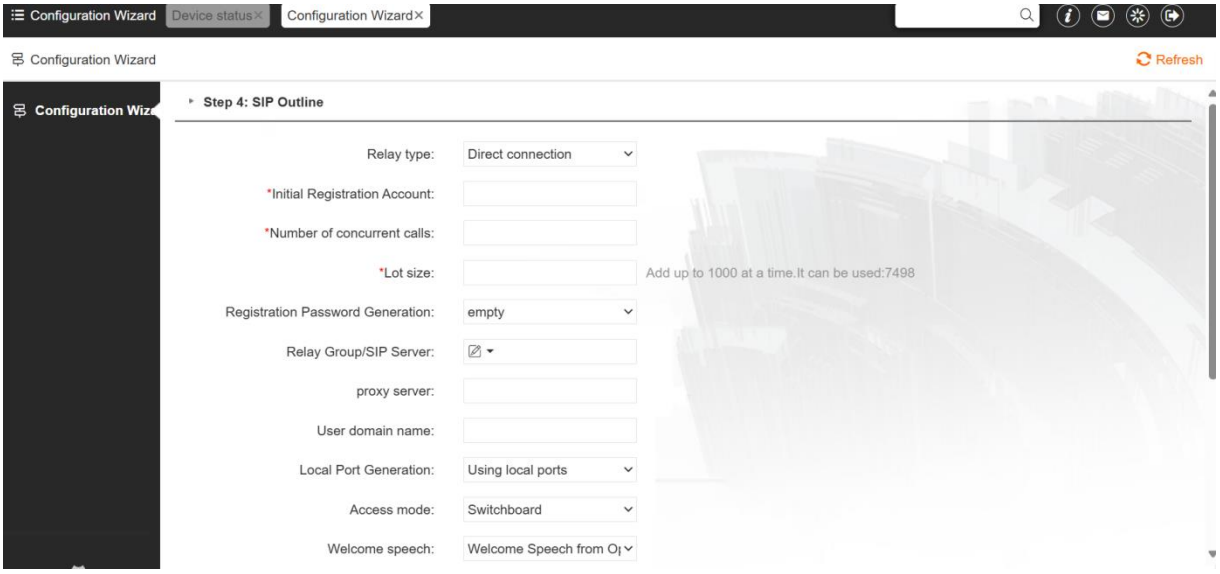
For a description of the parameters, see Table3.14 *This step can be skipped

 Copyright © Redstone Systems, Inc

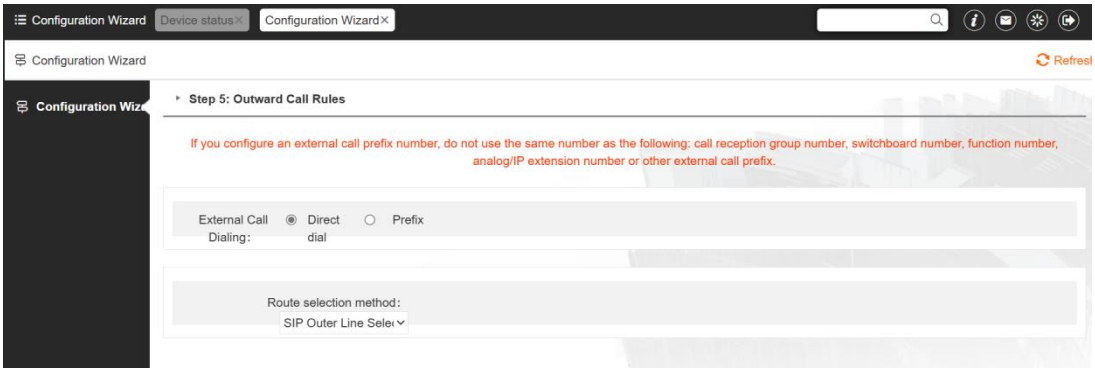
2.2.4 Step 4: SIP Outbound

For a description of the parameters, see Table3.20.

*This step can be skipped



2.2.5 Step 5: Outbound Calling Rules

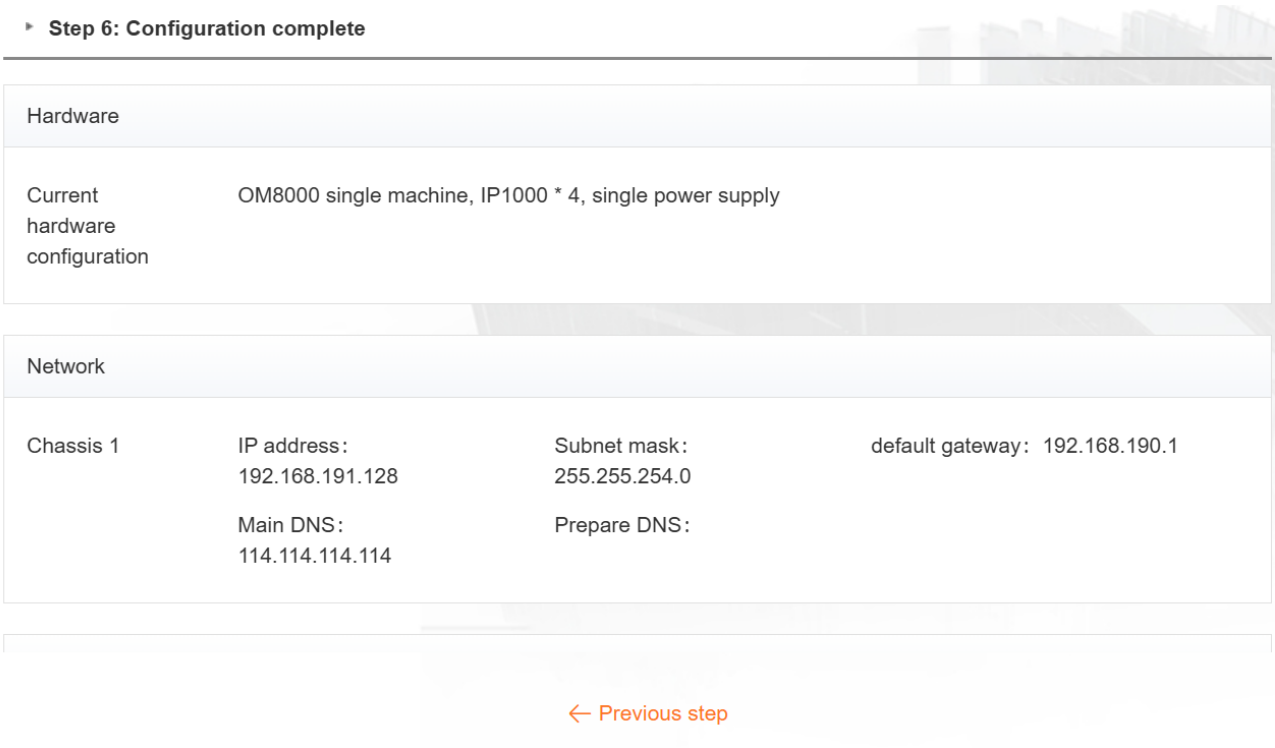


For a description of the parameters, see 3.2.2 Outsider Rule

*This step can be skipped

 Copyright © Redstone Systems, Inc

2.2.6 Step 6: Configuration Completed



After confirming that the configuration is correct, click "OK" to submit the previous configuration and complete the initial configuration.

 Copyright © Redstone Systems, Inc

3 Configure Personalization Features

3.1 Condition Monitoring

Status monitoring provides query on equipment status, extension status, outline status, and system status, which helps maintenance personnel to understand the status of equipment and troubleshoot problems in time.

Device Status: Real-time presentation of the current status of the device hardware, including indicator lights, board status, connectivity, power supply and so on.

Extension Status: presents the usage of the device's extensions, including the overall status as well as the status of each line.

Outline status: presents the usage of the device's trunk, including the overall status as well as the status of each outline.

System Status: presents the health of the system operation, including CPU, RAM, storage usage, fan, power supply, port status, and so on.

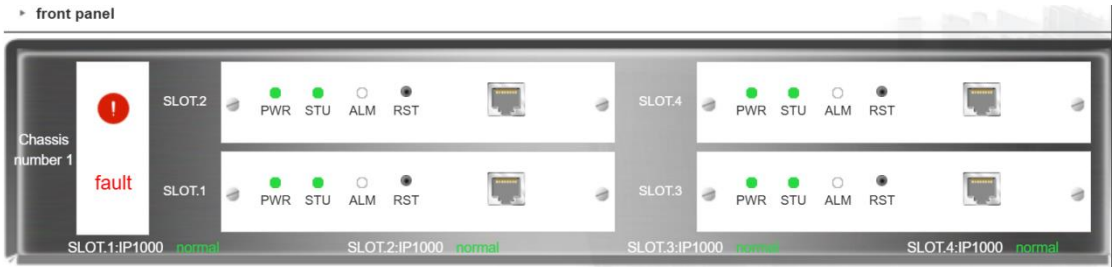
3.1.1 Device Status

Go to Status Monitor>Device Status to view.

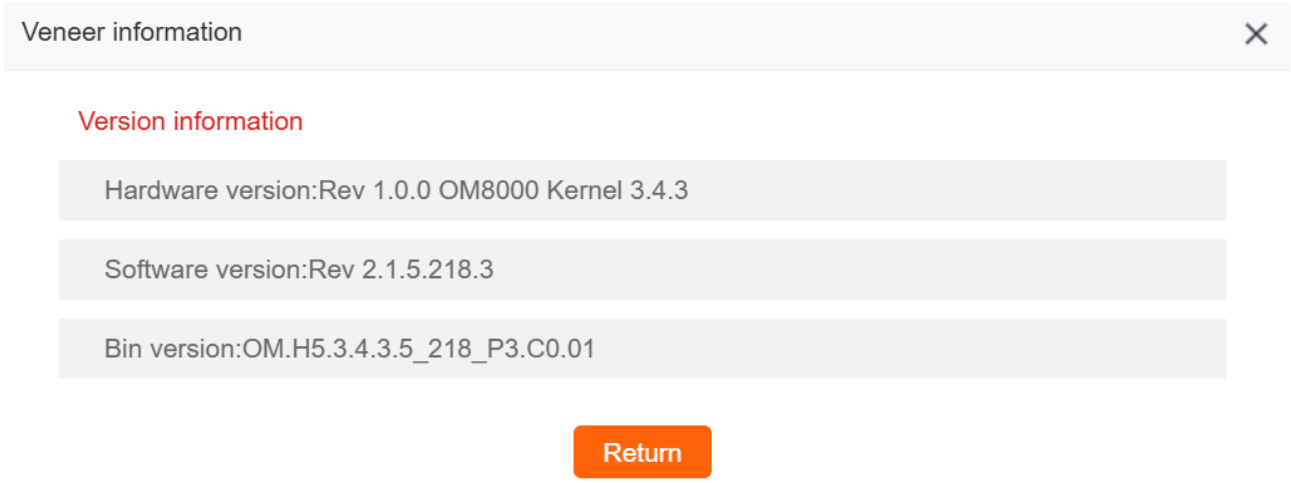
Front Panel

Displays the fan/sub-card status of the corresponding chassis.

 Copyright © Redstone Systems, Inc



Click on a sub-card to display the version information for that sub-card.



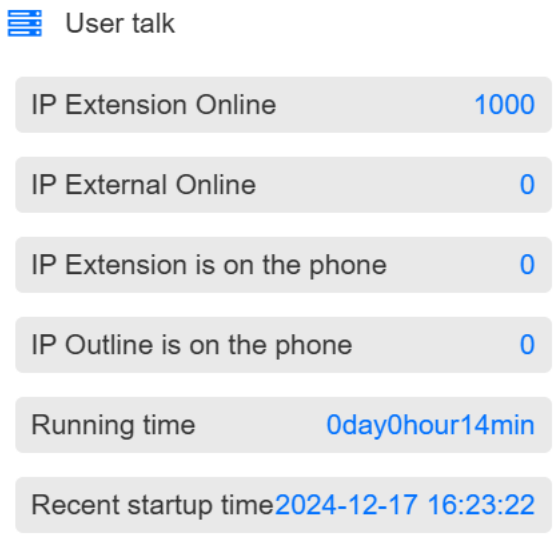
Rear Panel

Displays the chassis operating status, including indicators, sub-card status, and power status.



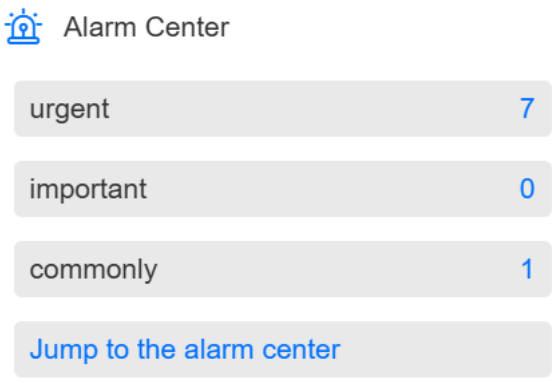
Subscriber Call

Displays extension and outline online status, call status, etc.



Alarm Center

Display the number of alarm messages by level. Levels include urgent, important, and commonly. Click "Jump to the alarm center" to view specific alarms.



Security Center

Displays security-related alarm class and configuration class information, click to view Specific items.

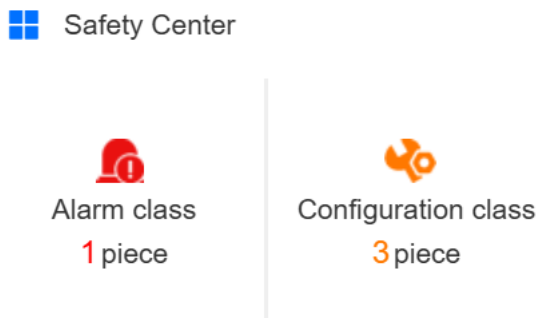


Table3.1 Description of Device Status

Item	Description
Alarm class	Subjected to a SIP attack
	Excessive international calling hours
	Illegal user SIP request
	SSH login password error
	SSH login
	Modify the SIP port
	Administrator Login
	IP address change
	Change administrator password
	Wrong login password
Configuration class	SSH service turned on
	The SIP service uses the default port 5060, it is recommended to change it to a port above 7000
	Currently there are XXX users with international long distance privileges, please open them carefully according to the actual situation.

 Copyright © Redstone Systems, Inc

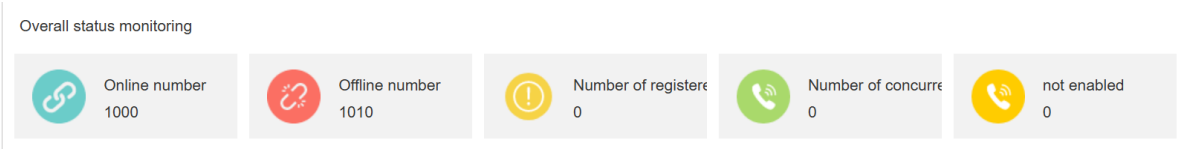
Item	Description
	There is no long distance call duration limitation, please go to "Long Distance Call Limitation" to configure.
	Default administrator password has not been changed

3.1.2 Extension Status

Go to Status Monitor>Extension Status to view.

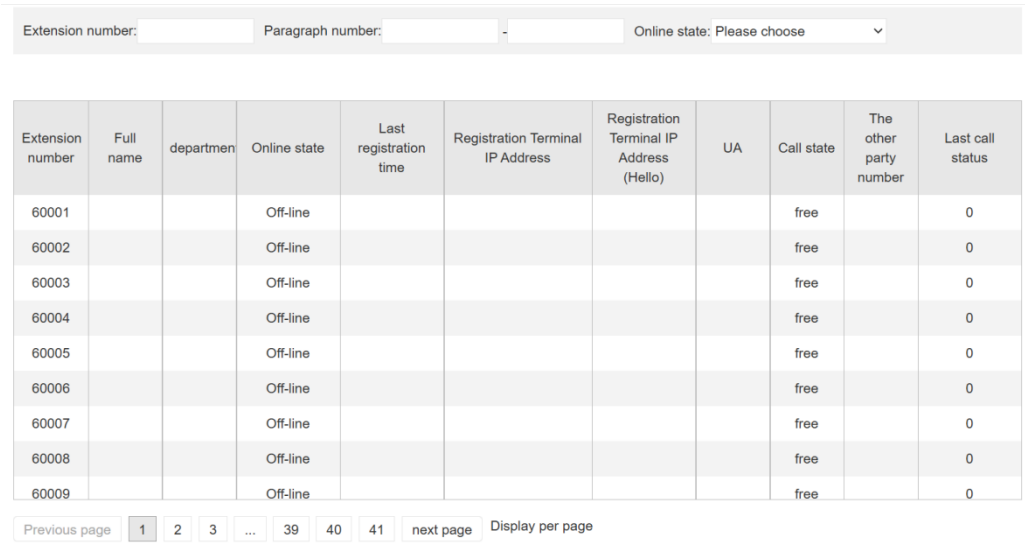
Overall Status Monitoring

Statistics on the number of extensions online, offline, registration exceptions, and call concurrency.



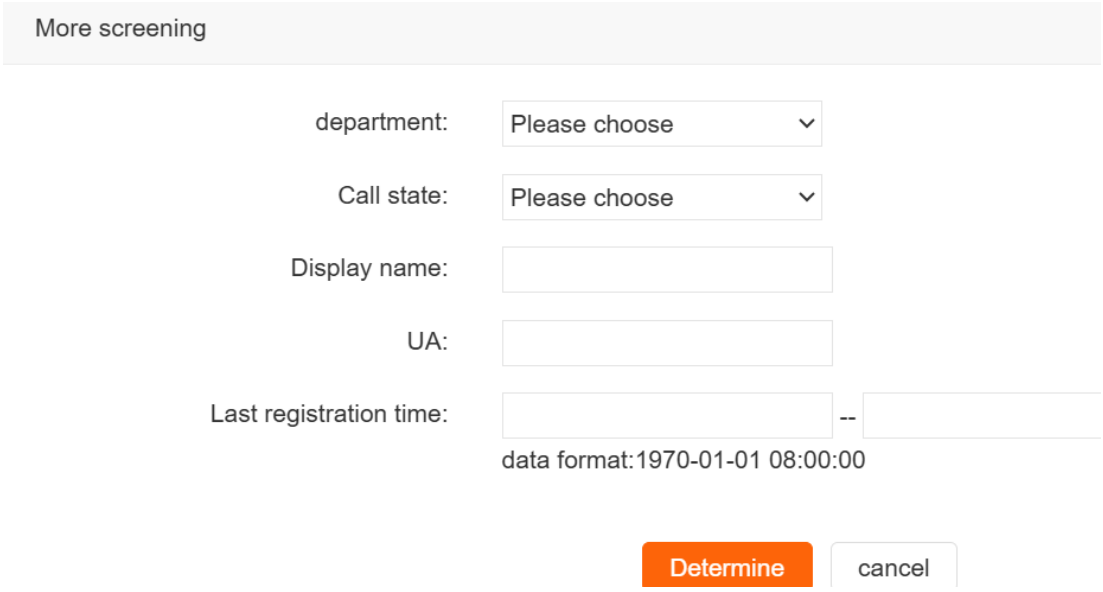
Detailed Data

Displays detailed information about each extension and allows you to filter the queried extensions based on multiple dimensions.



- Extension number: Enter the extension number and click "Query" to filter out the extension information.
- Paragraph number: Enter the number segment, click "Query", you can filter out all the extension information of the number segment.
- Online status: Divided into online (successful registration, IP address authentication), offline (registration failure, unregistered, logged out) two categories of a total of five options, can be used with the number, number with the number, accurate screening of eligible extension number.

Click "More Filters" to filter by department, call state, display name, UA, and last registration time.



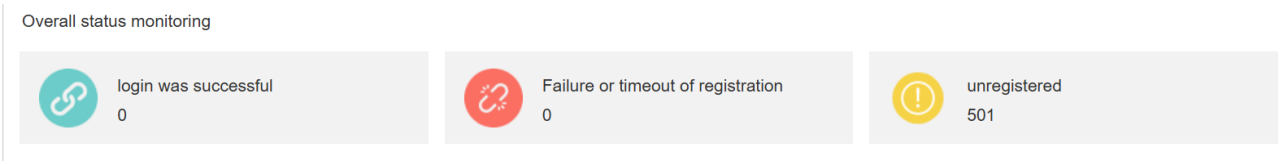
3.1.3 Outsider Status

Go to Status Monitor>Outside Line Status to view.

Overall Status Monitoring

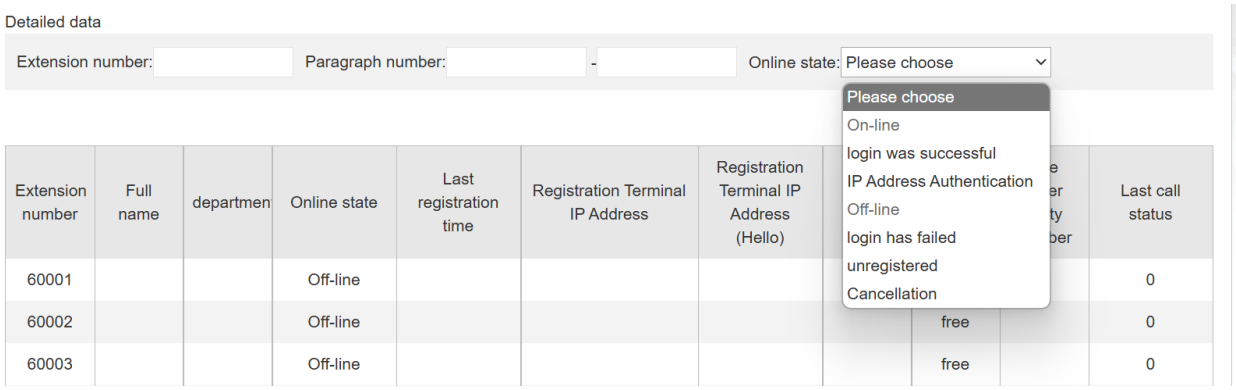
Statistics on the number of successful outline registrations, failed registration,

unregistered and calls in progress.



Detailed Data

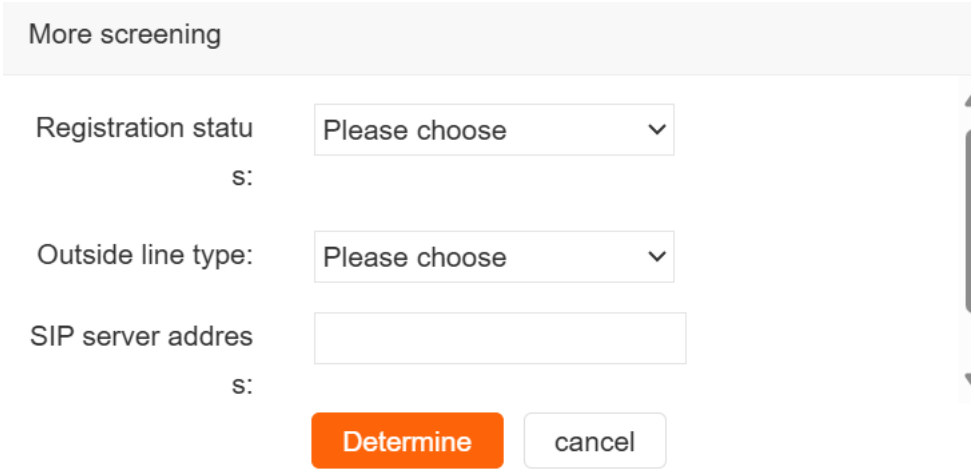
Displays detailed information about each outline and filter the queried outlines based on multiple dimensions.



- Outside line number: Enter the outside line number and click "Query" to filter out the information of the outside line.
- Paragraph number: Enter the number segment, click "Query", you can filter out all the outside line information of the number segment.
- Online status: divided into idle, inbound ringing, inbound call, inbound call, outbound ringback, outbound call, outbound call, etc. Multiple options are available, which can be matched with numbers and segments to accurately screen eligible numbers.

By clicking "More Filter", you can filter by registration status, outside line type, and SIP server address.

 Copyright © Redstone Systems, Inc



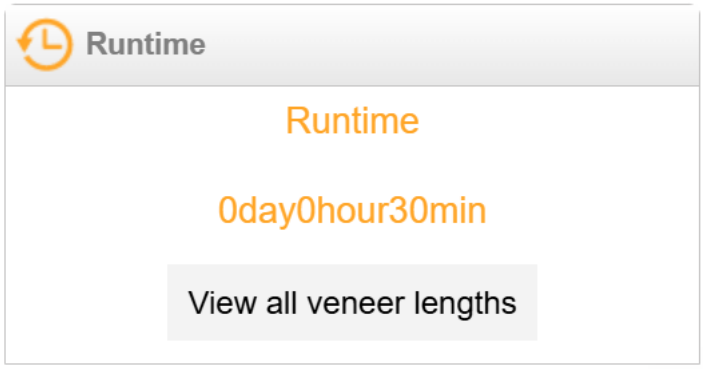
3.1.4 System Status

Go to Status Monitor>System Status to view.

Displays system information such as runtime, CPU usage, RAM usage, storage usage, network connection status, fan status, chassis temperature, power supply status, primary/standby status, and enabled service listening ports.

runtime

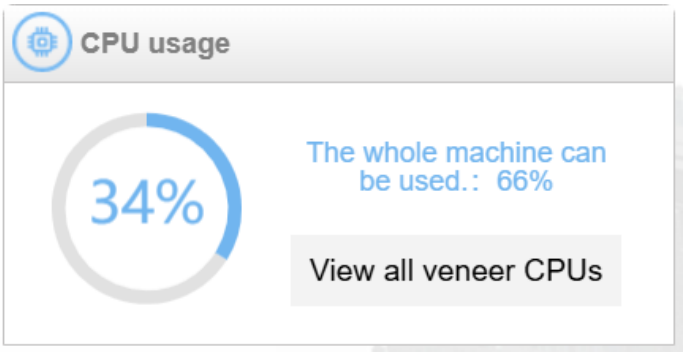
Displays the master board runtime. Click "View all veneer lengths" to display all board hours.



CPU Usage

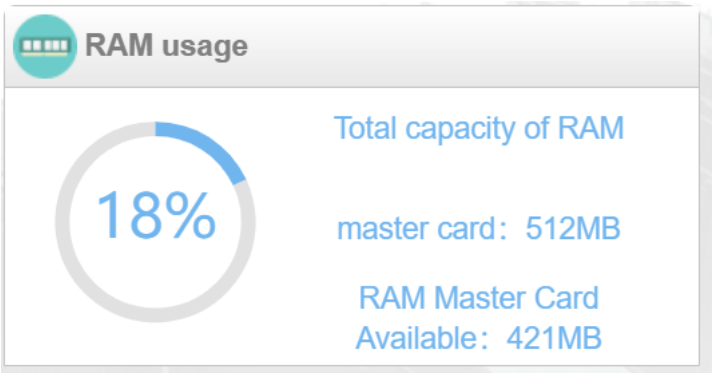
Displays the CPU occupancy rate. Click "View all veneer CPUs" to display the CPU utilization of all boards.

 Copyright © Redstone Systems, Inc



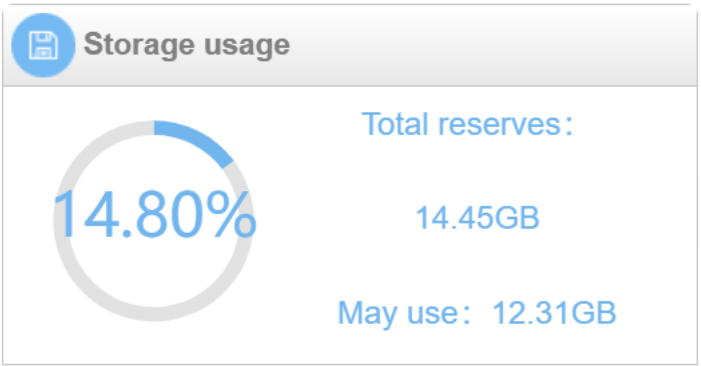
RAM Utilization

Displays the memory usage of the main board. Click "View All Single Board RAM" to display the memory usage of all single boards.



Storage Utilization

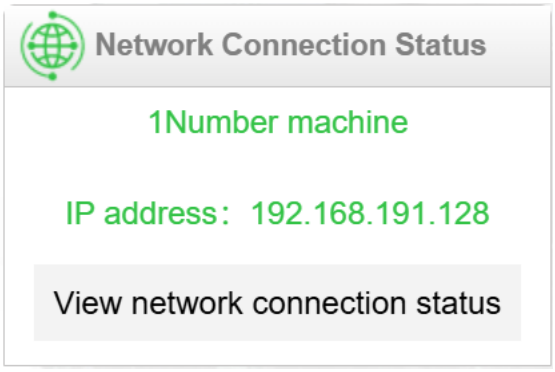
Displays the internal storage occupancy. Click "View All Chassis Storage" to display all chassis storage.



 Copyright © Redstone Systems, Inc

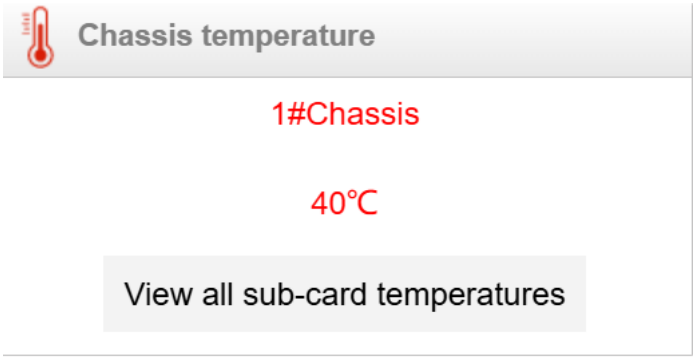
Network Connection Status

Displays the IP address of the chassis. Click "View network connection status" to display the network connection status.



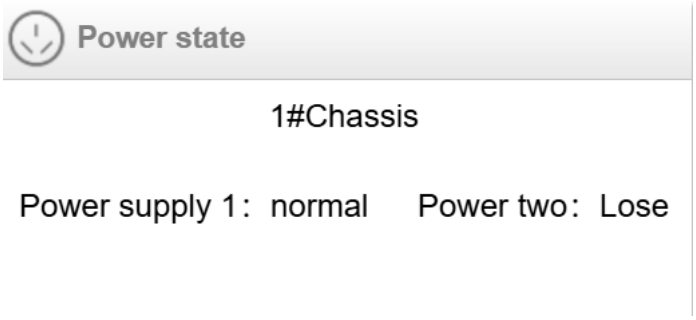
Chassis Temperature

Displays the chassis temperature. Click "View all sub-card temperatures" to display the temperature of each sub-card.



Power State

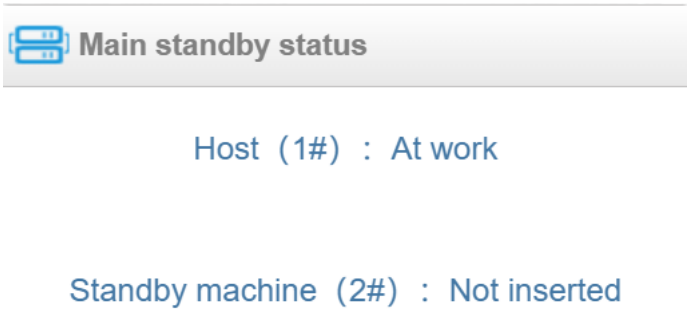
Displays the power supply operating status.



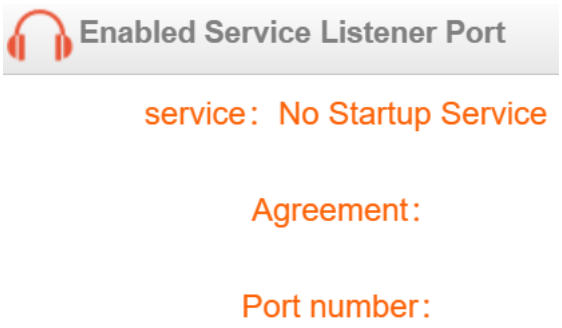
 Copyright © Redstone Systems, Inc

Primary/standby Status

Displays the primary and standby of both chassis. In the dual chassis state, one chassis is in operation and the other chassis is in standby.

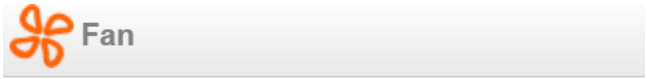


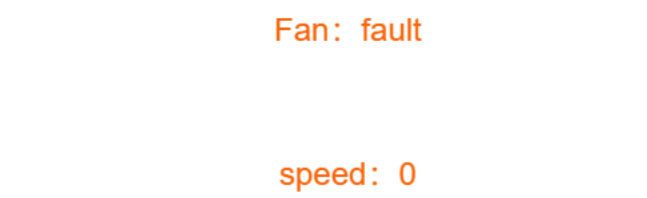
Enabled Service Listener Port



Fan

Displays the fan status.





 Copyright © Redstone Systems, Inc

3.2 Basic Settings

3.2.1 Network Setup

Equipment Name

Go to Basic setup>network configuration and configure the device name.

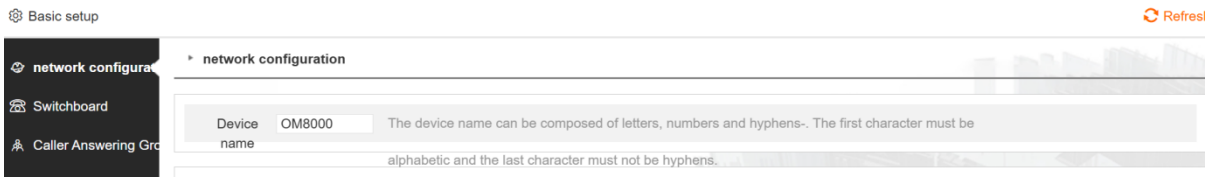


Table3.2 Description of Equipment Name

Item	Description
Device Name	The name of the device may consist of letters, numbers and the hyphen "-", the first letter of which must be a letter and the last letter must not be a hyphen.

Operating Mode

Used to set the operating mode of the network port ETH1/ETH2. The other two network ports of the REX8000, AUX1 and AUX2, are only used for interconnection between dual machines when double stacking.

Go to Basic setup>network configuration to configure it.

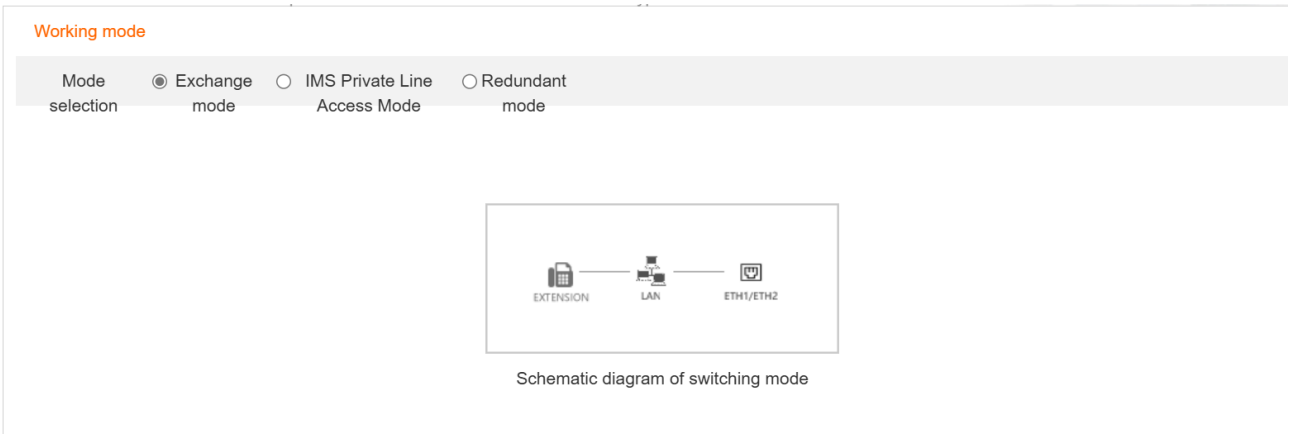
- Exchange Mode

The ETH1 and ETH2 interfaces are switch port and share the same IP address.

 Copyright © Redstone Systems, Inc

Figure3-1 switching mode

Single chassis



Dual chassis

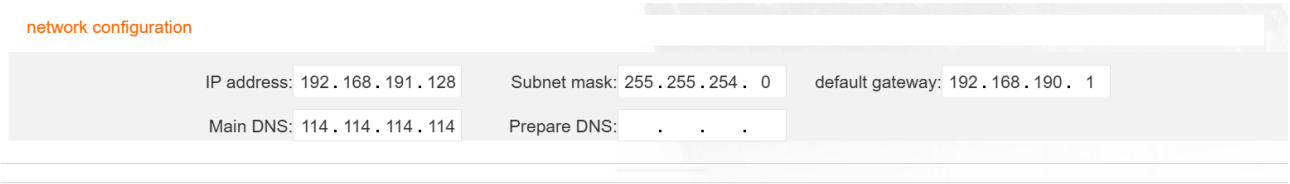


Table3.3 Parameter description

Item	Description
Single chassis	IP Address: The IP address of the device. Subnet Mask: The subnet mask is used in conjunction with the IP address. Default Gateway: The IP address of the LAN gateway where the gateway is located. DNS servers: Set the preferred and alternate DND servers. Prioritize the use of preferred DNS servers to resolve domain names
Dual chassis	IP address: Three addresses need to be configured, one for the whole machine, chassis 1 and chassis 2 respectively. The entire address is the device address that is reflected externally by the two chassis as a whole when dual-chassis stacking. The address of each chassis is used for dual interconnect or when accessing that chassis individually. Subnet Mask: Configuring the subnet mask of the whole machine. The subnet mask of chassis 1 and 2 is the same as the whole machine. Gateway address: Configuring the gateway of the whole machine. The gateway of chassis 1 and 2 is the same as the whole machine. DNS Servers: Set the preferred and alternate DNS servers. When the destination address accessed by the device is a domain name, it prioritizes the request to the preferred DNS server to resolve the domain name.

 Copyright © Redstone Systems, Inc

- IMS Private Line Access Mode

This mode allows you to configure an independent IP address for the ETH2. This mode is generally used to connect an ONU(Optical Network Unit)to access the carrier's dedicated voice network. If the API application and recording server are in the dedicated voice network, you need to check the corresponding option to use this network interface.

Single chassis



Dual chassis

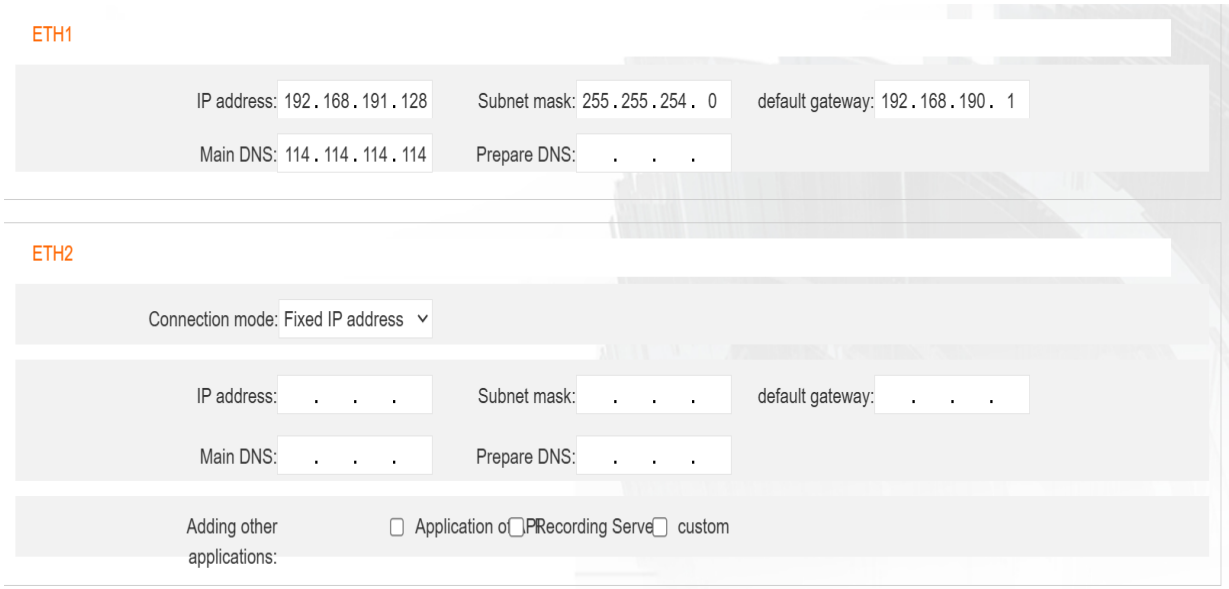


Table3.4 IMS Dedicated Access Mode Parameter Description

Item	Description
ETH1	
IP address	IP address of the network port ETH1.
Subnet mask	The subnet mask of the network port ETH1.
default gateway	Gateway IP address of the LAN to which the network port ETH1 is connected.
Main DNS	Enter the IP address of the preferred DNS server.
Prepare DNS	Enter the IP address of the alternate DNS server.
ETH2 (same ETH2 configuration for both chassis when dual stacked)	
IP address	IP address of the network port ETH2.
Subnet mask	The subnet mask of the network port ETH2.
default gateway	Gateway IP address of the LAN to which the network port ETH2 is connected.
Main DNS	Enter the IP address of the preferred DNS server.
Prepare DNS	Enter the IP address of the alternate DNS server.
Add other applications	API Application: If the API application server is within the voice private network, it needs to be checked. Recording Server: If the recording server is in the voice private network, you need to check the box. Custom: Addresses that match to a custom address segment automatically go to the voice private network.

- Redundant Mode

This mode is only applicable in the single chassis case.

Connect both ETH1 and ETH2 interfaces to the same LAN or WAN, prioritize the use of the ETH1 port, and when the ETH1 connection fails, the device automatically enables the ETH2 port.

 Copyright © Redstone Systems, Inc



802.1X

802.1X is an IEEE standard for authentication of users accessing a network, known as Port-Based Network Access Control (PNAC). 802.1X authentication involves three components: the applicant, the authenticator, and the authentication server. The applicant is a client device that needs to connect to a LAN/WAN, the authenticator is a network device (e.g., an Ethernet switch or a wireless access point), and the authentication server is usually a host that supports the RADIUS and EAP protocols.

With 802.1X, the applicant provides credentials, such as a username/password or digital certificate, to the authenticator, who forwards them to the authentication server for verification. If the authentication server deems the credentials valid, the applicant can access the network.

The REX supports 802.X and acts as an applicant, requiring 802.X to be enabled on the REX when the network requires 802.1X authentication.

Go to Basic Setup>Network Configuration to enable 802.1X.

Figure3-2 802.1X Configuration Interface

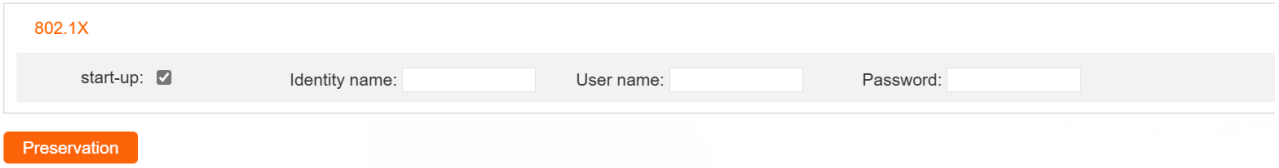


Table3.5 802.1X Interface Parameter Description

Item	Description
start-up	Enable the 802.1X function.
Identity name	Identity for authentication, provided by the authentication server
User name	Username for authentication, provided by the authentication server
Password	Password for authentication, provided by the authentication server

3.2.2 Outgoing Rule

Click Basic Setup>Outgoing Rule to configure the rules when an extension makes an outbound call.

Direct dial



Prefix

Click Add to add a prefix.

 Copyright © Redstone Systems, Inc

Table3.6 Outbound call rule parameter description

Item	Description
Outbound Dialing Method	Direct dialing: Extension users dial internal extension numbers and external numbers directly. Prefix: Extension users dial internal extension number directly. Add prefix to select outgoing line when dialing external number.
Selection Method	When the device is configured with multiple outgoing lines, you can select the outgoing call selection method according to the actual need. The device provides the following outbound call routing options: • SIP Outside Line Sequential Selection: Outgoing via SIP outside line, always select the first free line to call out according to the order of SIP outside line number. For example, the numbers 754321, 754322, and 754323 are filled in the Outbound field. 754321 is currently being used for outgoing calls, when another outgoing call is made then 754322 will be selected for outgoing calls. • SIP Outside Line Rotation: Outgoing via SIP outside line, take turns to select the free line to call out according to the order of SIP outside line number. For example, the numbers 754321, 754322 and 754323 are filled in the Outgoing line field, the last call is outgoing through 754321, at this time, another outgoing call will select 754322 to call out (when 754322 is idle), if 754322 is busy, 754323 will be selected to call out. Routing: using the routing table to set specific routing rules. For more information, please refer to 3.6.6 .
Prefix	Users can select the corresponding line selection method when dialing an outgoing line by using the outgoing call selection prefix configured here. For example, if the outgoing line selection prefix is set to 9 and the corresponding line selection method is set to SIP Outside Line Sequential Selection. User dials 9 before dialing an external number, the device selects the SIP outgoing line to call the other party according to the selection method. Note 1: This parameter is configurable only when the Outbound Dialing Method is Add Prefix. Note 2: The Outside Line Prefix cannot conflict with extension numbers, group numbers of Call Pickup Groups, feature codes and other Outside Line Prefix numbers.
Second Dial Tone	After the extension user dials the outgoing call prefix, the device provides a second dial tone to remind the user to dial the other party's number. Note: This parameter is configurable only when the Outbound Dialing Method is Add Prefix.
External Line	Specify the outgoing line number corresponding to the prefix, i.e., the corresponding outgoing line when selecting SIP outgoing lines for sequential and rotation selection. You can select the outside number directly or enter it manually, with comma "," separating each number. Indicates all available lines of the system when no line is specified.
Manipulate	Click it to make changes to the outbound call rules. When you're done making changes, click Save in the bottom right corner of the page.

 Copyright © Redstone Systems, Inc

3.2.3 Central Exchange

Automated Operator

The Auto Attendant feature is where the REXplays voice navigation (welcome message) to the caller after connecting an inbound call. Voice navigation in REX is divided into two categories: single-level voice navigation (subsequently referred to as a "voice file") and multi-level voice navigation (subsequently referred to as "multi-level IVR").

Note: The voice navigation configured in this section is the default voice navigation used by all outside lines. If you need to change the voice navigation for an outside line individually, you need to go to Outside Line Settings > SIP Outside Line to modify the configuration of the corresponding outside line.

Follow the steps below to configure the voice navigation used by the automated attendant:

Step1. Click Basic Settings>Switchboard to enter the Auto Attendant Configuration screen.

Step2. Split between working and non-working hours (default is Whole work).

Step3. Select the appropriate voice navigation for working hours and non-working hours.

Figure3-3 Auto Attendant Configuration Screen

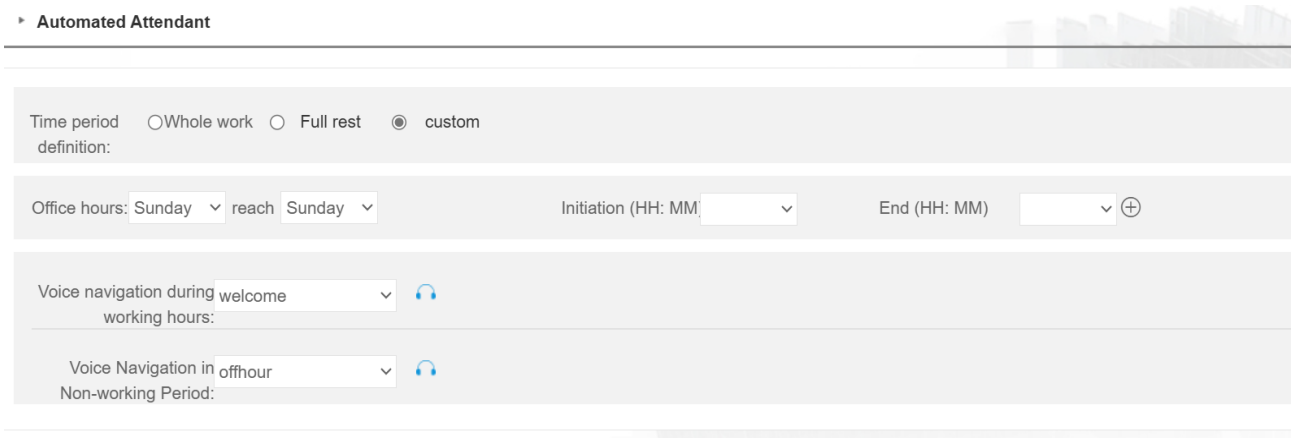


Table3.7 Automated Operator Parameters

Item	Description
Definition Of Time Slots	Whole work: Always play the work hour welcome message. Full rest: Always play the welcome message during non-working hours. Custom: Set the time range of the working hours during the week, and the hours outside the time range are non-working hours. Click + to define up to three work periods per day. After the definition is complete, external calls during the time slot are heard as working hour voice navigation, and times outside the time slot are heard as non-working hour voice navigation.
Voice Navigation During Working Hours	Select the voice navigation used for the work session from the drop-down list, either as a voice file or a multi-level IVR: • By default, the system has a voice file "welcome" as the voice navigation during working hours. • To set up a multi-level IVR, click Add IVR. For specific production see 3.2.4 . Click Audition to hear the current voice navigation content.
Out-Of-Hours Voice Navigation	Select the voice navigation used during non-working hours from the drop-down list, either as a voice file or a multi-level IVR: • By default, the system has a voice file "offhour" for non-working hours, if you want to change it.. • To set up a multi-level IVR, clickAdd IVR. For specific production see 3.2.4 . Click Auditionto listen to the current voice navigation content.

Step4. Save the settings.

Customizing and Replacing Voice Files

The device is shipped from the factory with two voice files by default, which are used as voice navigation during working hours and non-working hours.

Table3.8 Factory Default Voice File

Time Of Entry Into Force	Voice File Name	Element
Working Hours	welcome	Thank you for calling. If you know your party's extension, please dial it now or press zero transfer to an operator.
Non-Working Hours	offhour	Thank you for calling. Our office is closed. If you know the extension please dial it now.

You can also prepare voice files as follows.

- Upload an existing welcome message

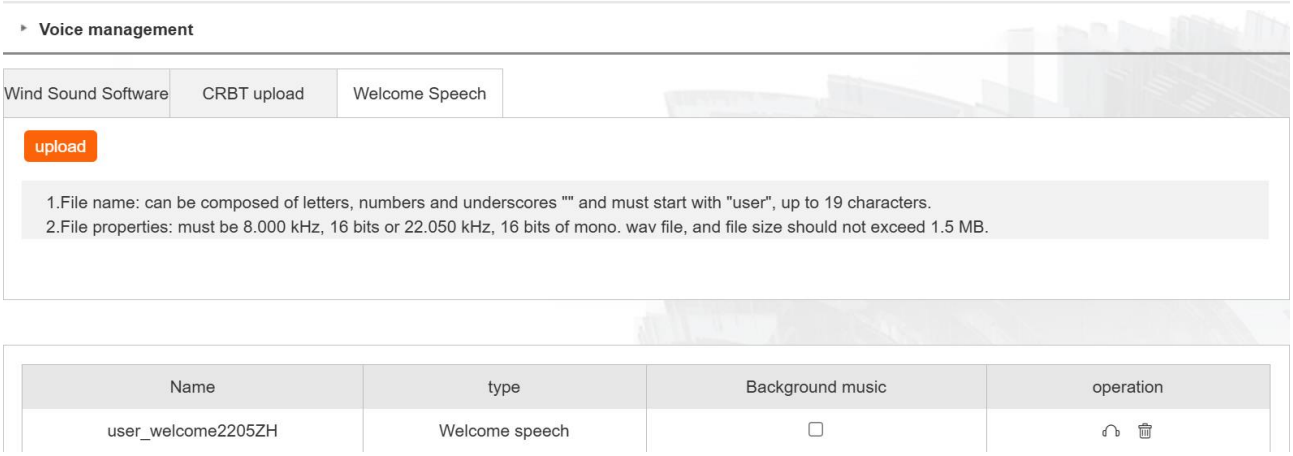
 Copyright © Redstone Systems, Inc

- Recording welcome message by phone

1) Upload Welcome Message

Step1. Click Basic Setup>Voice Management>Upload Speech.

Step2. Click Upload and select the eligible welcome message to upload.



2) Recording Welcome Message by phone

Welcome messages can be recorded directly via the shortcut keys on the handset. This method requires a phone connected to the device. It is recommended to record in a noise-free environment.

Table3.9 Microphone Recording Welcome Note

Item	Description
Sound Recordings	Off-hook the phone and dial *81, start recording after the voice prompt, and hang up directly after recording.
Listen	Off-hook the phone and dial *8200 to listen to the temporarily stored voice file.
Save	• Off-hook the phone and dial *8301 and then hang up to replace the work hour welcome message welcome; • Off-hook the phone and dial *8302 and then hang up to replace the non-working hour welcome message offhour.
Play the Welcome Messages Currently In Use	• Off-hook the phone and dial *8201 to hear the saved welcome message for working hour; • Off-hook the phone and dial *8202 to hear the saved welcome message for non-working hours.

 Copyright © Redstone Systems, Inc

Item	Description
Recovery	Off-hook the phone and dial *8300 to restore the replacement of the previous voice file.

Note

Do not reboot the device during voice recording.

Recording with IP extensions must ensure that PCMU/PCMA encoding is used.

Telephone Operator

After the outside caller user dials 0 (the default), the call is forwarded to the operator's extension for processing. Please note that in this section, the operator's extension is also known as the "switchboard", for example, the "switchboard" in the voice prompt "To switch to the switchboard, please dial 0" means to switch to the operator's extension.

To add an operator extension or modify other related information, follow the steps below to configure:

Step1. Click Basic Setup>Switchboard to configure items related to the Operator.

 Copyright © Redstone Systems, Inc

Table3.10 Operator Configuration Screen

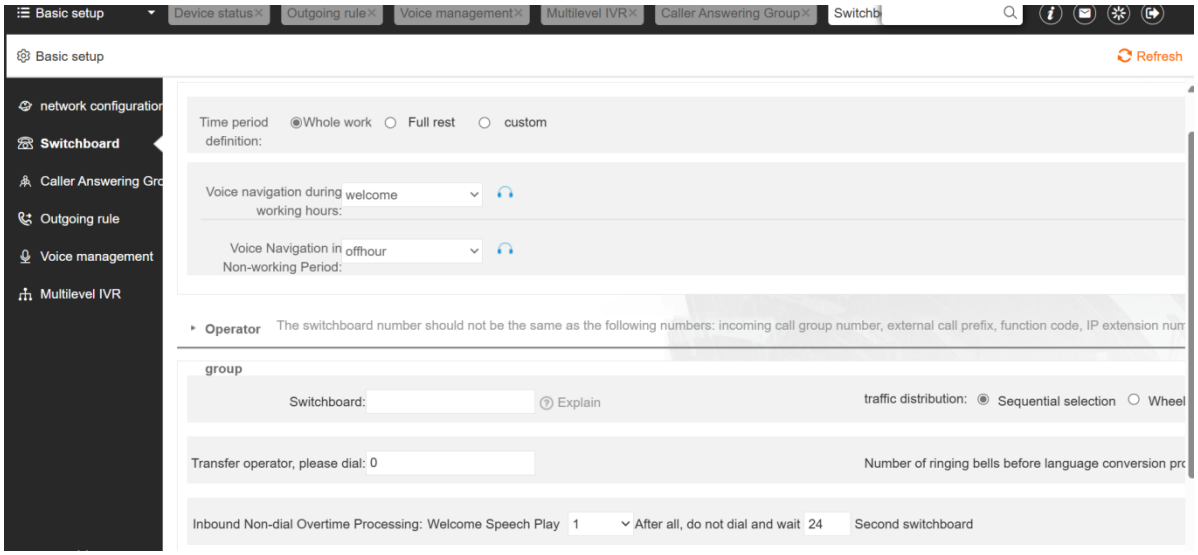


Table3.11 Operator Parameters

Item	Instructions
Switchboard	Fill in the extension number of the extension acting as an operator. Up to 5 can be set, use commas separating the numbers. Extensions filled in here automatically disable Call Waiting, Do Not Disturb, and Call Forwarding.
Traffic distribution	When there is more than one operator extension, you can select the call distribution method. ● Sequential Selection: Selects idle phones in the order of extension number entry in the switchboard input box. If the number filled in the switchboard is 321,322,323, the operator extension that is on the line is 321, and the next caller will choose 322 to ring. ● Wheel Selection: Take turns selecting phones in the order in which the extension numbers are entered in the switchboard input box. If the number filled in the switchboard is 321,322,323, and the operator extension that answered the call last time is 322, then the incoming call will choose 323 to ring, regardless of whether 322 is currently idle or not. ● Group vibration: All free operator extensions ring at the same time, and the first one to pick up is connected. Note: When the operator's extension is fully busy, incoming calls will enter the queue waiting (the queue allows up to 10 incoming calls to wait) and hear the voice prompts "Sorry, the switchboard is busy, to continue to wait, please press the * key, or change to dial another extension number".
Transfer operator, please dial	The number to be dialed when transferring to the switchboard, i.e., the switchboard prefix, which is 0 by default. If you change to another number, you will need to change the welcome message prompt accordingly.

 Copyright © Redstone Systems, Inc

Item	Instructions
Number of ringing bells before language conversion Prompts	When an outside caller dials an extension and the number of times the extension rings reach the set value (the default number is 10), the device plays a voice prompt to the caller.
Inbound Non-dial Overtime Processing	When an external call comes in, the device can play a welcome message to the calling party one or more times. After the welcome message is played, the device transfers the incoming call to the switchboard human operator at a predetermined time. The factory default is to play the welcome message once and then wait 24 seconds to transfer to the switchboard without dialing.

Step2. Save the settings.

3.2.4 Multi-level IVR

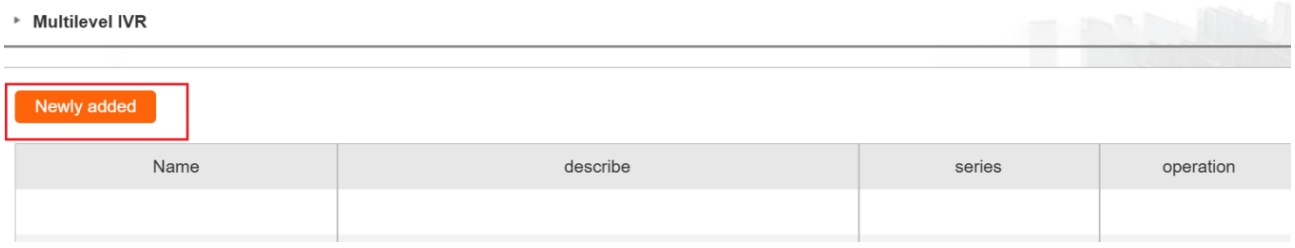
The multi-level IVR function allows inbound users to independently select the desired service through the handset buttons according to the broadcast content of the voice navigation menu. The following is an example of how to configure a multi-level IVR.

A shopping hotline is open 24/7 and the voice navigation consists of a secondary menu. After the user calls in, the first level menu allows the user to select "product ordering" or "technical consulting" business, the second level of the corresponding two menus respectively allow the user to further select "product ordering" and "technical consulting" under the sub-business. In addition, the user can choose to return to a previous menu, wait to be served by the switchboard, and dial an extension number directly during the interaction. The detailed IVR flow is shown below.

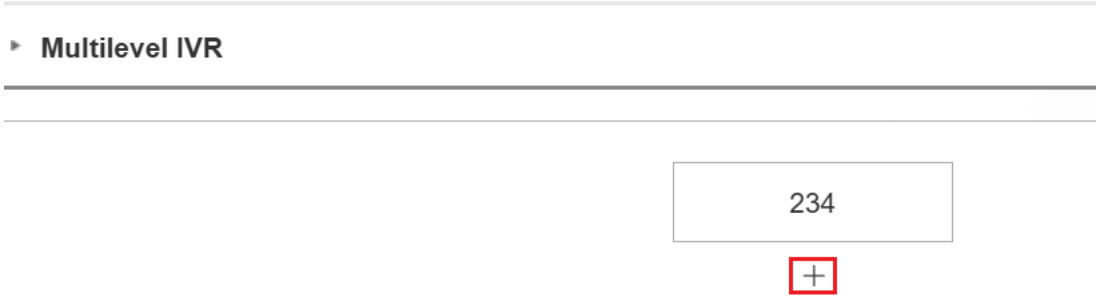
Step1. Go to Basic Setup>Multilevel IVR.

Step2. Click Newly added to enter the name and description of the multilevel IVR. The name consists of English characters, numbers, and hyphens. Allows the creation of multiple multi-level IVRs.

Step3. Click Save.



Step4. Click the Modify icon under "Operation" to enter the multi-level IVR definition interface.



Step5. Click on the + sign. Configure the parameters for this level of IVR when the following screen appears, and then click Confirm.

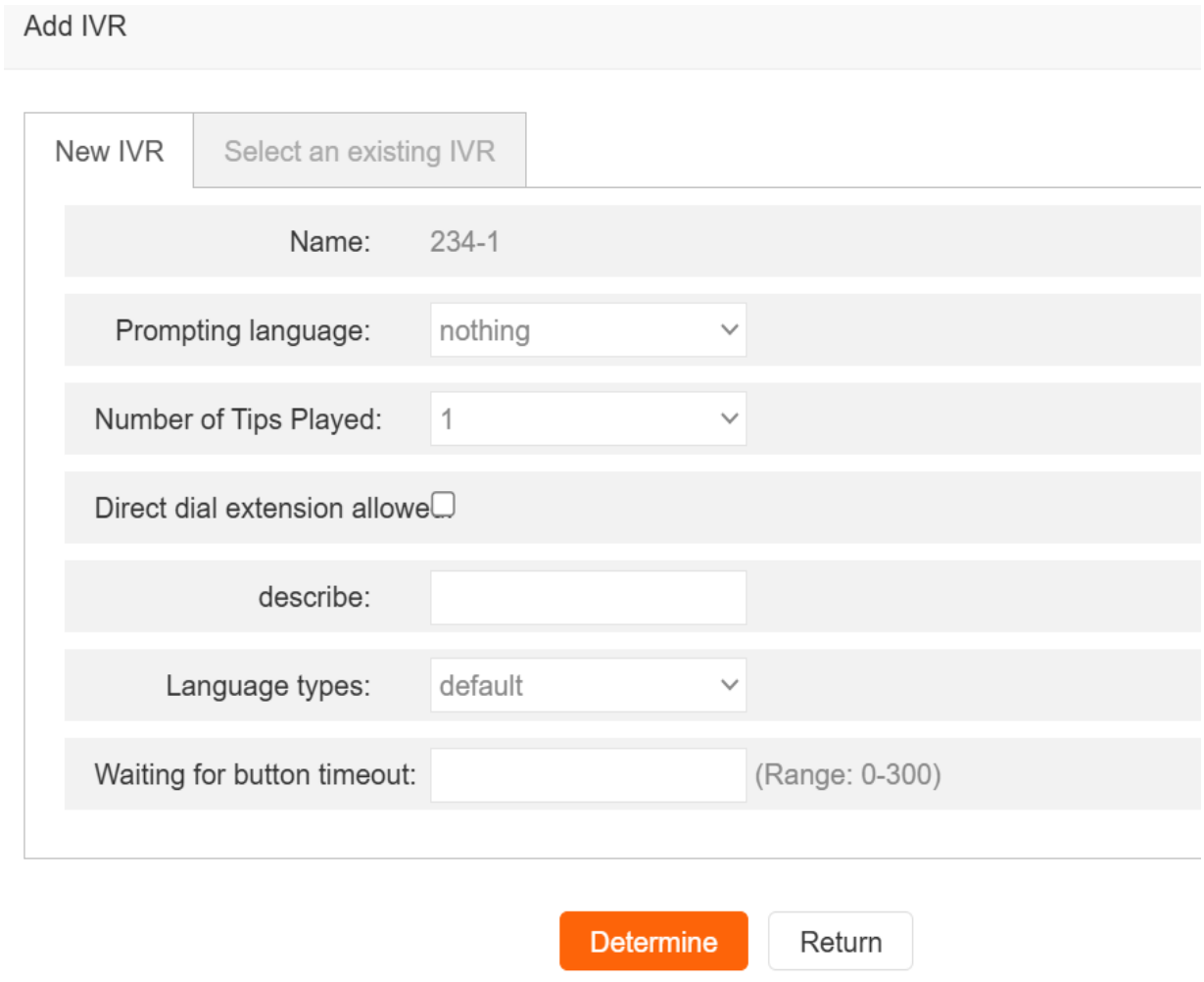


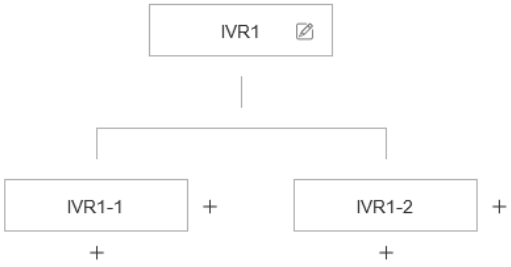
Table3.12 Multi-level IVR

Item	instructions
Name	Consists of letters, numbers, hyphens and underscores, and is no more than 20 characters long.
Describe	Describe the use of voice navigation at this level.

 Copyright © Redstone Systems, Inc

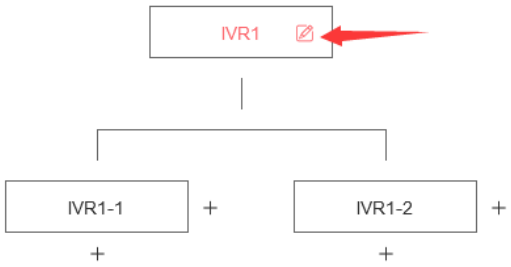
Item	instructions
Prompting language	Select a voice file for broadcasting. Voice files need to be prepared in advance.
Language type	For multilingual IVR. Only when multilingual voice navigation is broadcast at the first level, you need to select the corresponding language voice pack for each subsequent level.
Number of Tips Played	The number of times a voice file is played without the caller dialing. The default is 1 time.
Direct dial extensions allowed	When checked, dialing an extension number is allowed during voice file playback.
Waiting for button timeout	The user does not dial the timeout period after the voice file has been played a sufficient number of times, the default is 3 seconds.

Step6. Click the + on the right to add a leveled IVR. Click on the + below to add the next level of IVR. Repeat the configuration of the previous step until all levels of IVR are configured.



Step7. Click Save.

Step8. Click to the right of each level name to expand the detailed configuration screen.



Step9. Configure specific events in the Detailed Configuration screen.

 Copyright © Redstone Systems, Inc

Figure3-4 IVR1 Configuration Interface

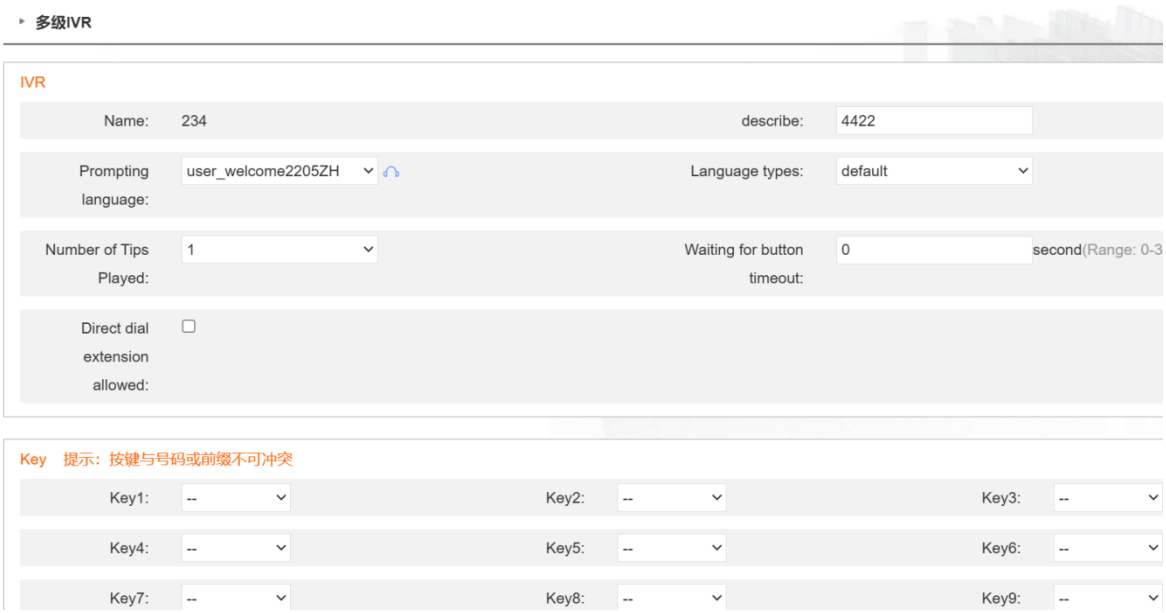


Table3.13 Multi-level IVR

Item	Instructions
Event	Press the button: ● Key 0~9, *, #: Processing after the user dials the number keys 0~9 or the * key or the # key. ● Press any key: defines the handling of other arbitrary keys under this menu. ● Timeout Processing: The user does not dial after the voice prompt for this menu is played until after the timeout has elapsed. The key corresponds to the operation: ● Transfer to Switchboard: Transfer to the switchboard operator, whose extension number is assigned in advance in the Basic Settings > Switchboard page. ● Hang up: ends the call. ● Transfer to Extension: Transfer to an extension, the specific extension number is selected via a drop-down menu or entered manually. Note: If you are transferring to an extension of a networking device, you can only enter the extension number manually. ● Transfer to Extension Group: Transfer to an extension group, the specific extension group number is selected by drop down arrow or manually entered. The extension group (call answering group) must be configure in advance in the Basic Setup>Call Answering Groups page. ● IVR: Go to the lower level IVR menu and select the name of the menu that has been added to the IVR list by using the drop down arrow. ● Broadcast Voice: Plays the voice file specified here.

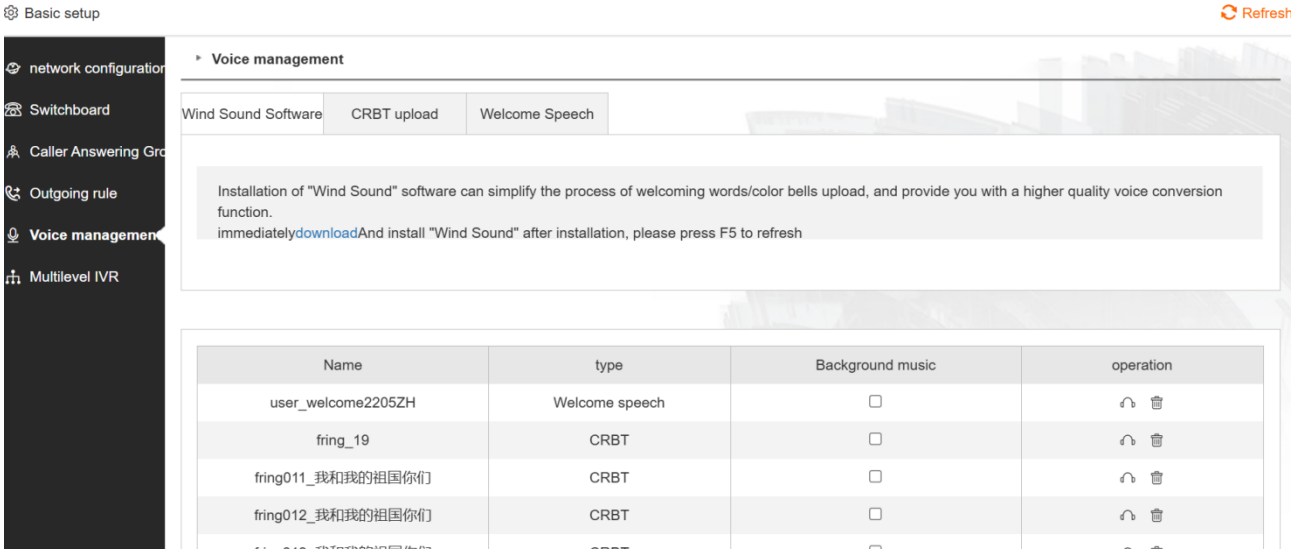
 Copyright © Redstone Systems, Inc

3.2.5 Voice Management

Wind Sound Software Upload

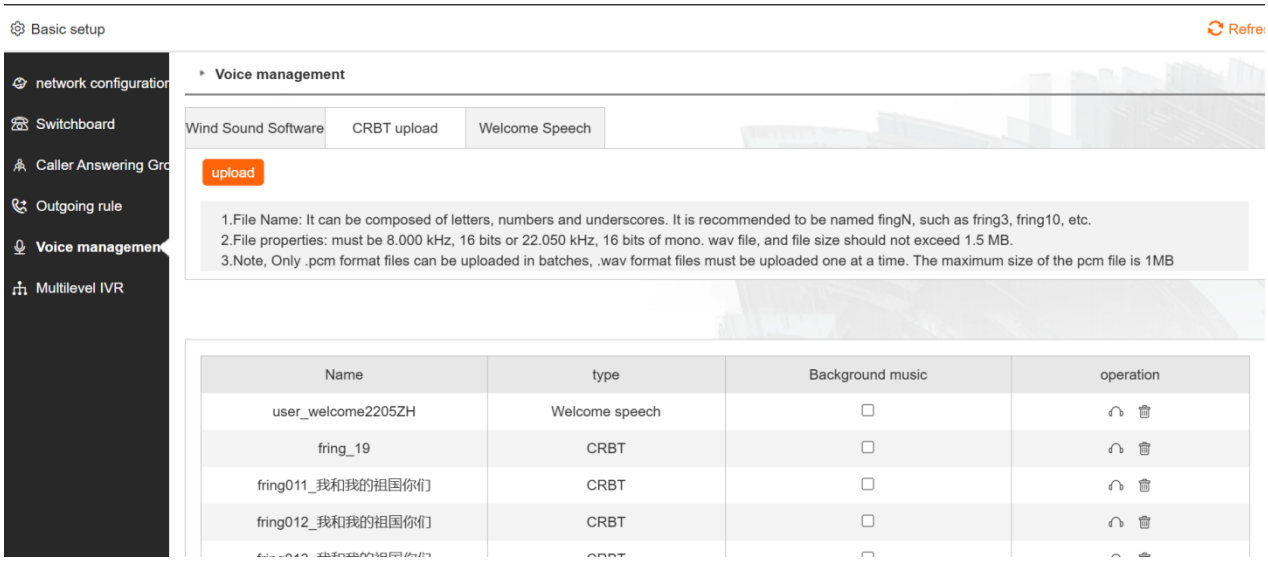
We recommend downloading and installing the "Wind Sound" software. When the format of the voice files for ringtones and welcome messages does not meet the requirements, you can use the "Wind Sound" software to convert the format, and then upload the voice files in the "Ringtone Upload" and "Welcome Message Upload" pages. page to upload voice files for ringtones and welcome messages.

Click Basic Setup>Voice management>Wind Sound Software, click Download, and install the software manually after the download is complete.



 Copyright © Redstone Systems, Inc

Ringtone Upload



Step1. Click Basic Setup>Voice management>CRBT upload, click Upload and select a voice file from your computer to upload. If the uploaded file has the same name as the original file in the system, the newly uploaded file will overwrite the original file.

The name and format of the uploaded voice file must comply with the requirements. Voice files are uploaded and stored in the built-in storage (path is /media/sda1/ann), as long as there is enough space in the built-in storage, there is no limit to the number of voice files that can be uploaded.

Step2. Click Extension Settings > IP Extension, click the extension corresponding to the to set the desired color ringtone for the extension.

Click to try out the colorful ringtones.

Step3. Click Save.

Color ringtone voice files can also be used to set up background music, see the following section.

Background Music (BGM)

Background music is the music that the device plays to the waiting party while the call is on hold, and all waiting parties hear the same music. The device ships with two built-in files that can be set as background music, fring2 and NewMorning, and users can also upload their own voice files.

The color ringtone voice file and background music voice file of the device can be common, the uploading steps refer to Color Ringtone Upload Uploading steps refer to Uploading Color Ringtone.

After uploading the customized voice file, the steps for setting the background music are

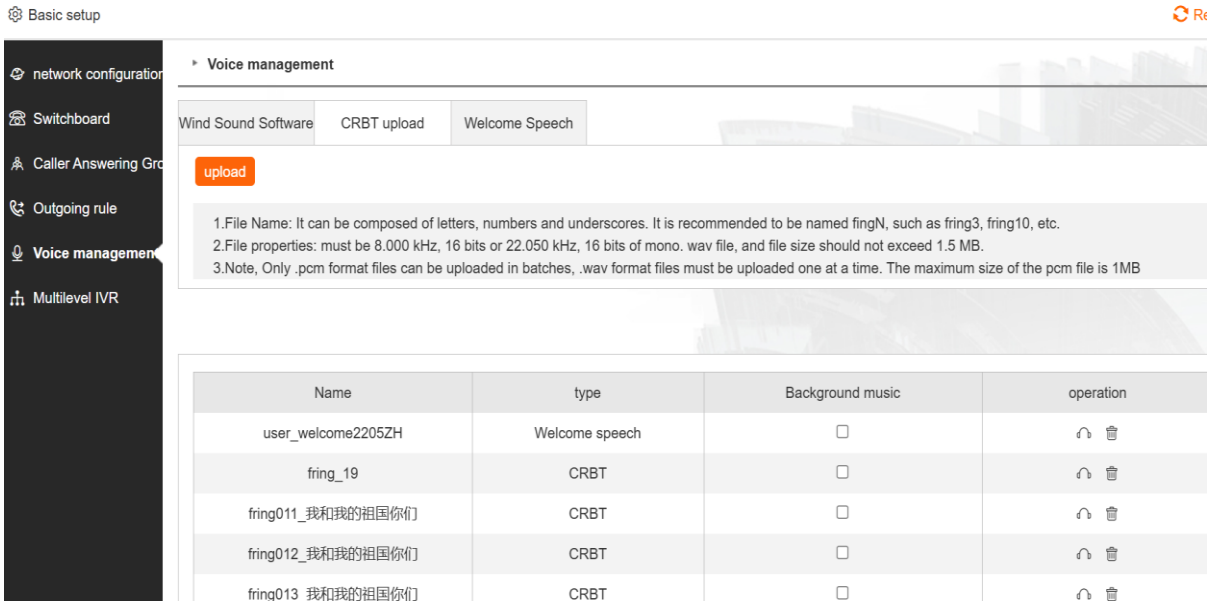
as follows:

Step1. Go to Basic Setup>Voice management>CRBT Upload, check the voice files that need to be set as background music, and confirm to save.

Click Audition to try the audio.

Click in the audio file list to delete the corresponding audio file.

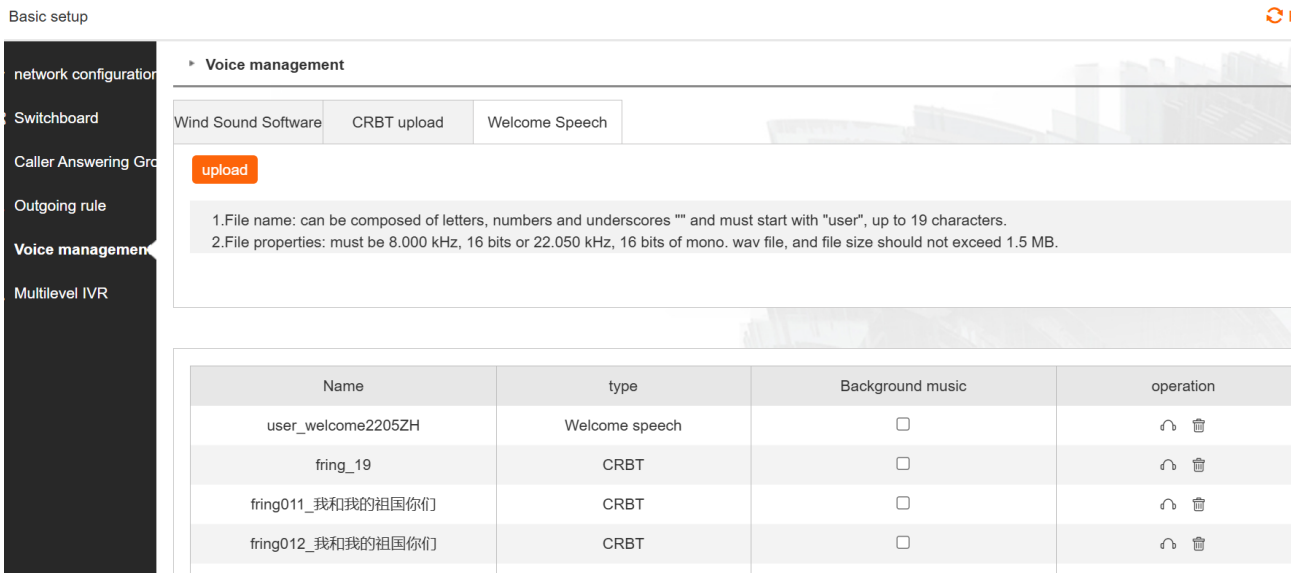
Figure3-5 Background Music Configuration Interface



Welcome Message Uploaded

Click Basic Setup>Voice management>Welcome Speech.

The uploaded file must fulfill the requirements in the page.



3.3 Extension Setup

3.3.1 IP Extension

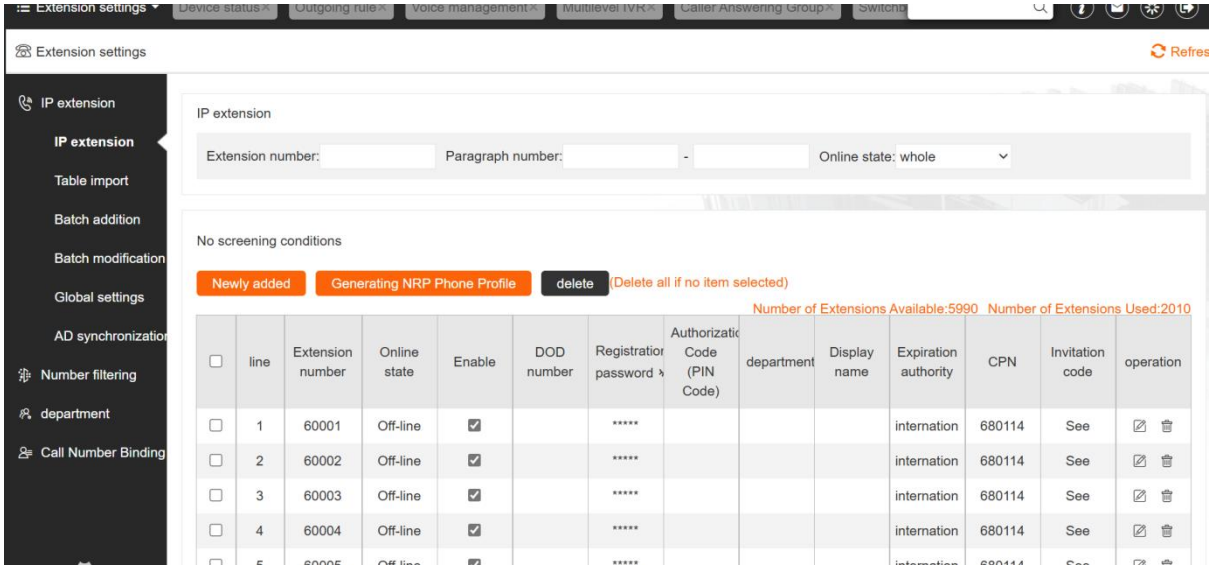
Extension List

IP Phones or Softphones (SIP phone software installed on a computer or cell phone) can be used as IP extensions after registering to REX.

To use IP extensions, you need to configure the extension account and registration password on the REX first.

The configuration steps for adding and configuring extension accounts one by one are as follows:

Step1. Click Extension settings > IP extension > IP Extension and click Add.



Step2. Enter the extension number, registration password, etc.

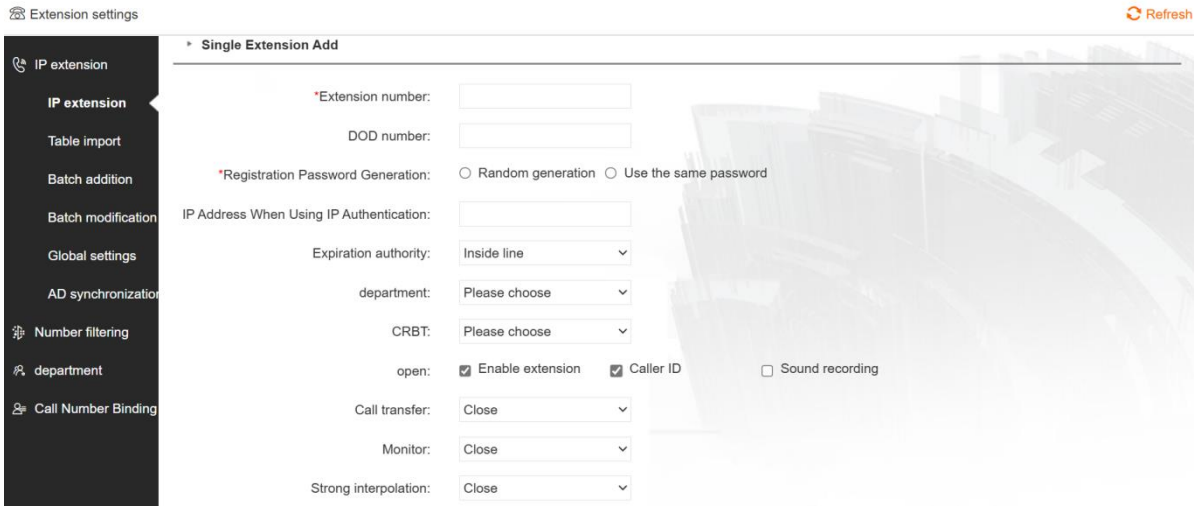


Table3.14 IP Extension Configuration Parameter Description

Item	Description
Extension Number	Extension number. Note: All extension numbers cannot be duplicated, nor can extension numbers be duplicated with outside numbers.
Registration password	The password used for extension registration. Generate or assign a random password.
IP Address When Using IP Authentication	When the REX8000 is bi-directionally reachable with the IP address of an extension, after entering the address of the IP extension into the REX, the REX will recognize the SIP endpoint from that address as a trusted endpoint, so that the IP extension can establish a SIP session with the REX without registration. This function is recommended when the REX is used in conjunction with a companion voice gateway. Fill in the IP address of the voice gateway here, and the address of the REX8000 on the voice gateway also needs to be filled into the proxy

Item	Description
	server, and set the subscriber line number of the gateway to the extension number on the REX8000.
Call-Out Authority	Calls made from an extension are restricted by outbound privileges. When a user outbound call exceeds permissions, the device will reject the call and play a voice prompt. If extension A's calling privilege is an internal line, when it calls local, domestic and international calls, you will hear the voice prompt: Sorry, your current calling privilege is an extension, please contact the administrator if you need to adjust it. The default is domestic. • Intercom: Allows internal calls to be made. • Local Calls: Allows to make internal calls and local calls. • Domestic: Internal calls, local calls and domestic long-distance calls are allowed. • International: Allows internal, local, domestic and international calls. • Prohibited: Only receiving calls is allowed.
Department	Select a department for the extension, and extensions within the same department can use the Group Pickup function to pick up calls on each other's behalf.
Authorization Code (Pin)	This password is used for authentication during *33 and *99 external inbound calls. Note 1: The *33 and *99 features allow users to perform telephone operations after calling in from outside the device. Note 2: The Call Authorization Code uses the same password as the extension lock, which is also used to set up the IP Phones to automatically download setup information.
Extension Lock	Check the checkbox to lock. Locked extensions can only dial internal lines; calling external lines requires authorization code (PIN) authentication.
Display Name	Configure the display name of the extension (Display Name), which supports Chinese and English. Displaying names only applies to extension interdialing and requires the IP extension to support name display. If both the REX and the IP phone terminal are configured with a display name, the name configured on the REX takes precedence.
Call-Out Authority	Calls made from an extension are restricted by outbound privileges. When a user outbound call exceeds permissions, the device will reject the call and play a voice prompt. If extension A's calling privilege is an internal line, when it calls local, domestic and international calls, you will hear the voice prompt: Sorry, your current calling privilege is an extension, please contact the administrator if you need to adjust it. The default is domestic. • Intercom: Allows internal calls to be made. • Local calls: Iternal calls and local calls are allowed. • Domestic: Internal calls, local calls and domestic long-distance calls are allowed. • International: Allows internal, local, domestic and international calls. • **Prohibited**: Only receiving calls is allowed.
Mobile Telephone Number	After entering a cell phone number, you do not need to enter a password for verification when using the *33 and *99 functions when calling into the device with

 Copyright © Redstone Systems, Inc

Item	Description
	that number. If the Dial *33 for external call function is also checked, after dialing the device's outside number from this phone, you can directly use the device's resources to make an outside call without entering *33.
Dial *33 for external call	Allows a preset cell phone (e.g., an employee cell phone) to make outbound calls through the device without entering a feature code after calling into the device's outside line. ● When checked, the cell phone number entered in the cell phone number beforehand, the outgoing line of the inbound device can directly dial the other number outbound when it hears the dial tone. ● When unchecked, you need to dial *33 first when this cell phone calls into the device's outside line and hear the dial tone before dialing the other party's number. Note: *33 is the default function code, which can be modified in Advanced Settings > Function Code page.
Caller Ring-Back Tone (CRBT)	Select the caller ring back tone of the extension, please refer to the uploading and management of caller ring back tone files. Ringtone Upload Please refer to Uploading Caller Ring Back Tones.
Extension Activation	If this item is not checked, the current account is not available.
Caller ID	With Caller ID turned on, when an outside line calls an extension on the REX, the calling number is displayed on the extension. It's not turned on, it's not displayed.
Sound Recordings	Record each call in its entirety. Note: The realization of this function requires that the recording function of the device is turned on, and the specific settings for recording can be referred to 3.5.3 .
Call Transfer	The device can transfer incoming calls to a specified phone or voice mailbox. The default is off. • All incoming calls to another phone: The device transfers all incoming calls from an extension to a specified phone. This function cannot be set for the switchboard operator extension. • Transfer to another phone when unable to answer: When the extension is busy or there is no answer, the device transfers the incoming call to the specified phone. • Transfer to another phone when busy: When the extension is busy (occupied), the device transfers the incoming call to the specified phone. • Transfer to another phone when there is no answer: When the extension does not answer, the device transfers the incoming call to the specified phone. • All calls to voicemail: the device transfers all incoming calls from the extension to voicemail. • Transfer to voicemail in case of busy/no answer: When the extension is not answering or occupied, the device transfers the incoming call to voicemail.
Distinguish Between Busy/No Answer Transfers	When the call transfer mode is transfer to another phone when no answer, you can set the target number for busy transfer and the target number for no-answer transfer individually when Distinguish Busy/No-Answer Transfer to Number is

 Copyright © Redstone Systems, Inc

Item	Description
to A Number	checked.
Transfer to Number/Busy Transfer to Number/No Answer Transfer to Number	When the call forwarding mode is transfer all incoming calls to another phone/transfer to another phone when unable to answer/transfer to another phone when busy/transfer to another phone when there is no answer, you need to enter the transfer target number, which can be filled in with the extension number or an external phone number (e.g., cell phone number, fixed-line phone, etc.). Transferring to an external phone requires the extension to have corresponding outbound privileges, and the external number needs to be prefixed with an outgoing prefix and separated by a comma.
Indentation Dialing Group	Reduced-digit dialing allows users to replace actual numbers with pre-set two-digit numbers, providing a convenient, easy-to-remember dialing method. For example, using 20 as the abbreviated code for 13823218765, simply dial **20 when making a call. Reduced digit dialing group consists of "Reduced Digit Code - Phone Number" (e.g. 20-13823218765), the range of the reduced digit code is 20~49, and a maximum of 30 groups can be configured, each group is separated by ",".
Hotline	The device automatically calls the hotline number after off-hook. • Off: Turns off the Hotline function. • Immediately: The device automatically dials a pre-set hotline number immediately after off-hook. • Delay: If the user does not dial the number within a certain period of time after off-hook, the device will automatically call the hotline number. The delay time defaults to 5 seconds. The REX's web interface can only set up hotline functions for analog extensions. Hotline functions for IP extensions need to be set up on the IP phone.
Numbers	Enter the hotline number.
Simultaneous Number	The device transfers incoming calls to your extension and another pre-programmed answering terminal (e.g., cell phone) at the same time. You can fill in the REX's extension number or external number, etc. Notes: • When Do Not Disturb, Unconditional Call Forwarding, and Secretarial Extension are turned on, Simultaneous Oscillation does not take effect. • If an incoming call is on hold, co-oscillation does not take effect. Co-oscillation to external terminals via an analog external line, which needs to support reverse polarity signals. If the external line does not provide a reverse polarity signal, the unit will ring the extension first, with a no answer timeout before sending the incoming call to the external terminal.
Rejected Caller Id	Users can fill in the numbers they don't want to answer here and the device will play a busy tone alert to the caller. If you fill in more than one number, please separate them with ",". Note: Extensions can call numbers in this list normally.
Secretarial Extension	By tying an extension to a secretarial extension, calls to that extension will be routed to the secretarial extension and answered by the secretary. You can go to Application Services>Secretary to check the secretarial method as needed:

 Copyright © Redstone Systems, Inc

Item	Description
	• Outside calls from this device to Secretary: Forward outside calls from this device to the Secretary's phone. • Incoming Calls from this device extension to Secretary: Forward calls from this device extension to the Secretary's phone. • Incoming Calls from Other Sites to Secretary (Group Network): Forwards all calls (both extensions and outside lines) from other devices in a multi-point group network to the secretary's phone. You can turn the secretary function on/off with the handset function code *35.
Monitor	Off: Prohibit this extension from monitoring other extension calls Global: Allows this extension to monitor calls from any extension under the device. In-group only: Allow this extension to monitor calls of any extension in the same department. Note: If one of the extensions on both sides of the call has enabled Listening Blocking, listening will not take effect.
Strong interpolation	OFF: Prohibits this extension from forcing calls to other extensions. Global: Allows this extension to force a call from any extension under the device to form a multi-party call. In-group only: Allow this extension to force insertion of the same department any extension to form a multi-party call. Note: If one of the extensions on either side of the call has strong interpolation blocking turned on, strong interpolation does not take effect.
Prohibition Of Substitution	When an incoming call on an extension is not answered, other extensions can answer it on behalf of the extension. Turning on this function prohibits incoming calls to this extension from being answered on behalf of other extensions. Note: The function of answered other extensions on behalf of this extension can be used without additional settings.
Call Waiting	The user will hear a beep when there is a new incoming call. At this point the user has three options: • Ignore new calls: continue the current call without doing anything. After a certain period of time, the "beep" will disappear automatically. • Answer a new call: Press ** on the handset to put the current call on hold (the other party listens to waiting music) and answer the new call. • Toggle Caller: Press ** to put the current call on hold and continue the call with the previously party. Note: Before using this feature, make sure Call Hold is turned on.
No forcible interposition	When this feature is turned on, calls from this extension are not allowed to be forcefully inserted.
Call Hold	You can pause the current call to put the other party on hold with background music and make a new call without hanging up.
Called Transfer	The current call can be forwarded to other extensions or external phones when this extension is the called one. For incoming calls to be forwarded to an outside telephone, this extension needs to have the Transfer Outside privilege. • Blind transfer: The current call is transferred directly to a third party (other internal extensions only), and the number of the transferred party (original caller) is

 Copyright © Redstone Systems, Inc

Item	Description
	displayed on the third party's phone. • Consultation transfer: A third party (an internal extension or an external phone) is dialed and a call is established, then the call is transferred and the third party displays the number of the intermediary transferor. Note: Before using the transfer feature, make sure Call Hold is turned on.
Call Forwarding	This extension can transfer the current call to other extensions or external phones when it is acting as a caller. For incoming calls to be forwarded to an outside telephone, this extension needs to have the Transfer Outside privilege. • Blind transfer: as above • Consultation transfer: as above Note: Before using the Call Forwarding feature, make sure Call Hold and Call Forwarding is turned on.
Forbidden to be monitored	When this feature is turned on, calls from this extension will not be allowed to be monitored.
Call Display in Call Waiting	The extension turns on Call Waiting, which displays the caller's number if another call comes in during the call.
Transfer external line	Check this box to allow this extension user to forward external incoming calls to a third-party cell phone or landline. Note 1: To realize the transfer external function, the extension must also have the corresponding outgoing call authority. Note 2: When transferring an external incoming call to an external third party, you will take up two outside lines and incur outgoing call charges. Administrators need to be cautious when turning on this feature.
Distinctive Ringing	The device selects the ringing method for analog phones based on the type of incoming call: • Internal caller:"Beep-Beep-Beep-Beep-Beep" • Incoming external phone call:"BeepBeep-BeepBeepBeep" Incoming call from a reduced-digit dialing number:"BeepBeepBeepBeepBeep-Beep-Beep"
Call limit	The device can be timed to turn off the outbound and inbound capabilities of an extension based on a preset timer. For specific settings, please refer to 3.5.4 .
Allow Phone Setup	Instant Recording: Allow extension users to press *# at any time during a call to record the current call; or dial *# before dialing the other party's number and then dialing the phone number to turn on the recording of the call. Recording specific settings can be found in 3.5.3 . Do Not Disturb: When checked, the extension user can set Do Not Disturb (Do Not Disturb can be enabled/disabled on the handset with function code *72 or via *99).

Step3. Save the settings.

 Copyright © Redstone Systems, Inc

Extension Table Import

For easy configuration, REX8000 supports batch import of multiple extension accounts via Excel (up to 1000 extensions at a time), eliminating the need to configure them one by one.

Click Extension settings > Table import to download the template and populate the information before importing.

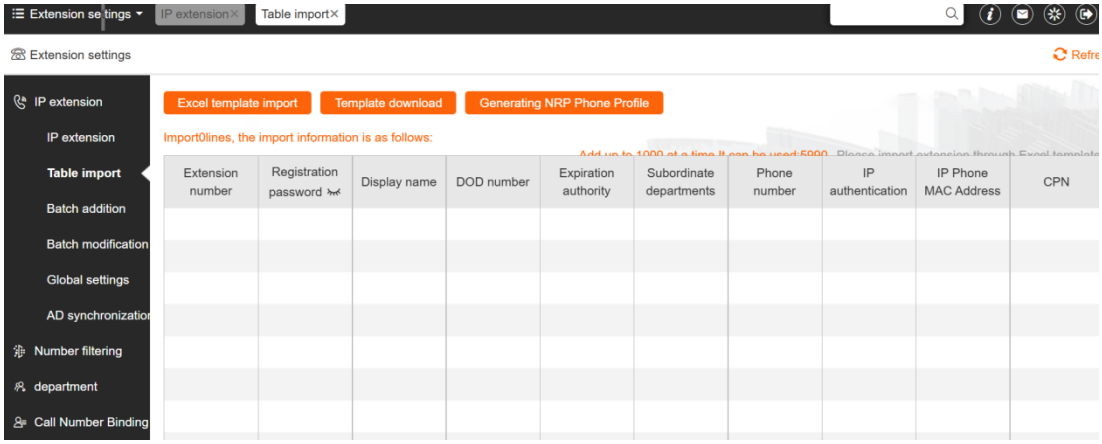


Table3.15 IP Extension Configuration Parameter Description

Item	Description
Excel Template Import	Click Excel Template Import and select the prepared template. When the import is complete, the table below shows the imported extensions.
Template Download	After downloading the template file for import, open the template and fill in the extension information in the format shown in the template.
Generating NRP Phone Profile	Clicking this button generates an IP phone profile in the device backend for the opening deployment of extension numbers for high volume IP phones. Note: All extension numbers cannot be duplicated, nor can extension numbers be duplicated with outside numbers.

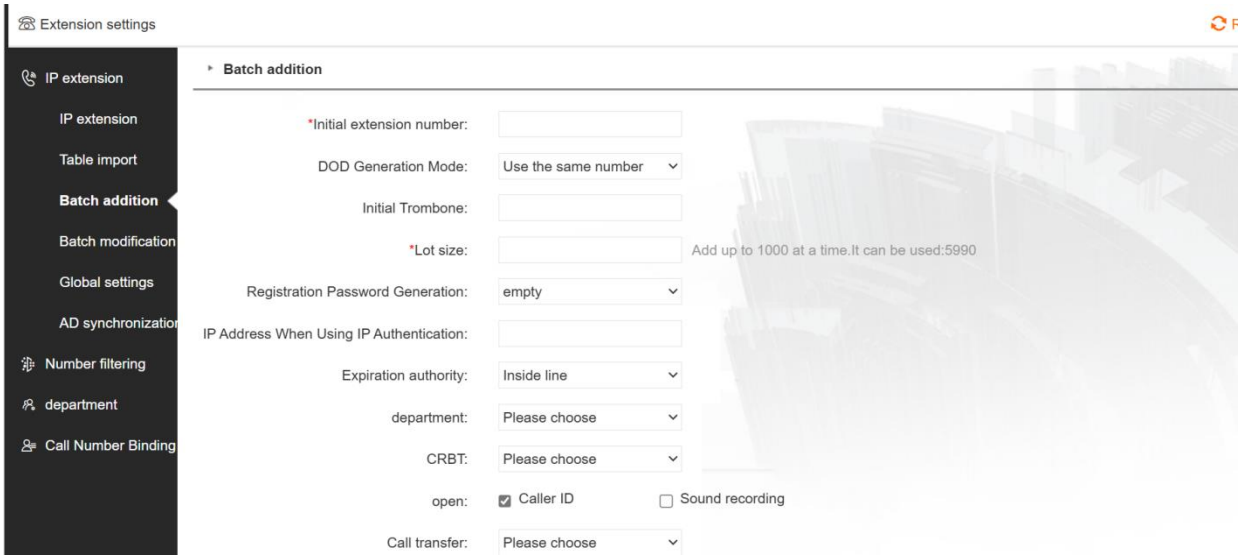
Extension Batch Add

For easy configuration, REX8000 supports batch creation of extension accounts, and all extensions created in a batch have the same features enabled. If different functionality is

 Copyright © Redstone Systems, Inc

required, it will need to be modified again separately. Supports batch creation of up to 1000 extension accounts at a time.

Click Extension settings > Batch addition, enter the starting extension number and the number of batches, select the features you want to enable, and click OK.



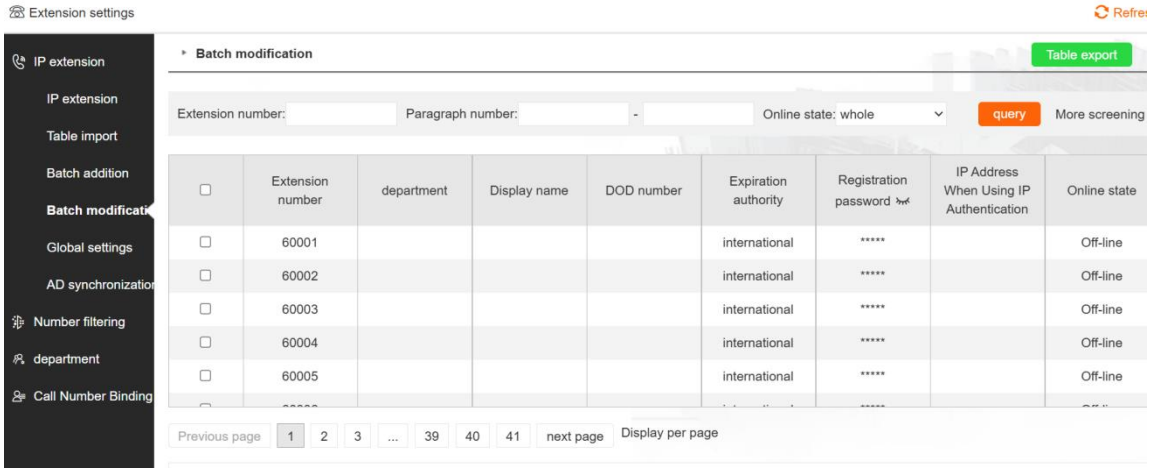
Extension Batch Modification

For easy modification, REX8000 supports batch modification of extensions.

Direct Modification

Click Extension settings>Batch Modification to filter the extension numbers you want to modify, and then select these extension numbers to modify the configuration in batch. Click OK after making the changes.

 Copyright © Redstone Systems, Inc

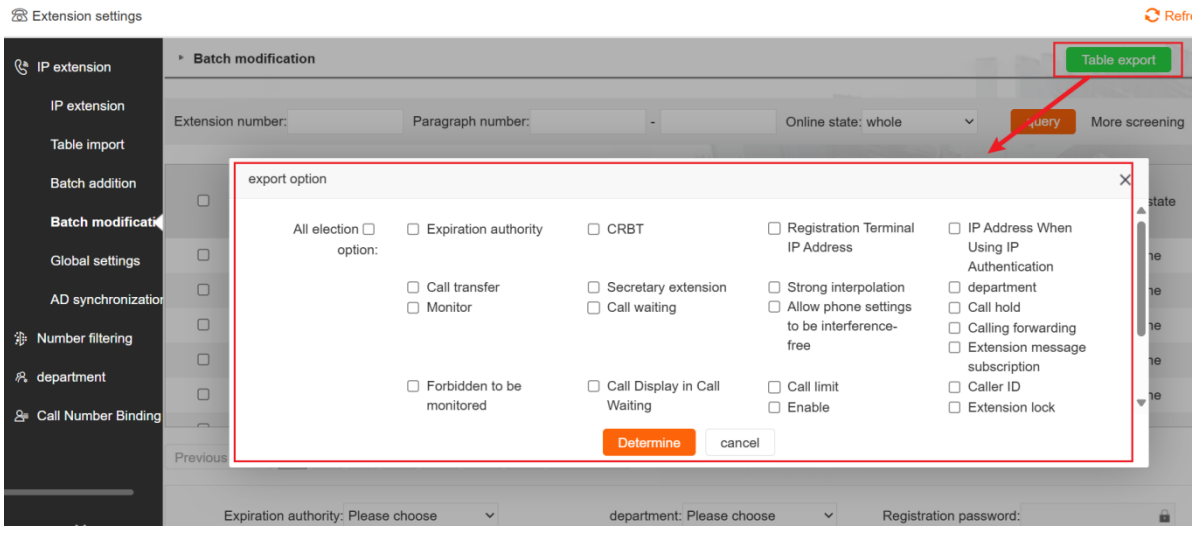


Modify after exporting the table

For easy modification, REX8000 supports batch modification of extensions by exporting Excel sheet.

Step1. Click Extension settings > Batch Modification.

Step2. Select the extensions that need to be modified, click Table export, and check or uncheck the features that need to be modified in the pop-up dialog box.



Step3. Click OK to download the Excel sheet.

Step4. Modify the configuration of the extension in the Excel sheet and save the file.

Step5. Click Form Import and after importing the configured file, it prompts for successful configuration.

Extension Global Settings

Go to Extension settings>IP Extension>Extension global settings and click OK after setting.

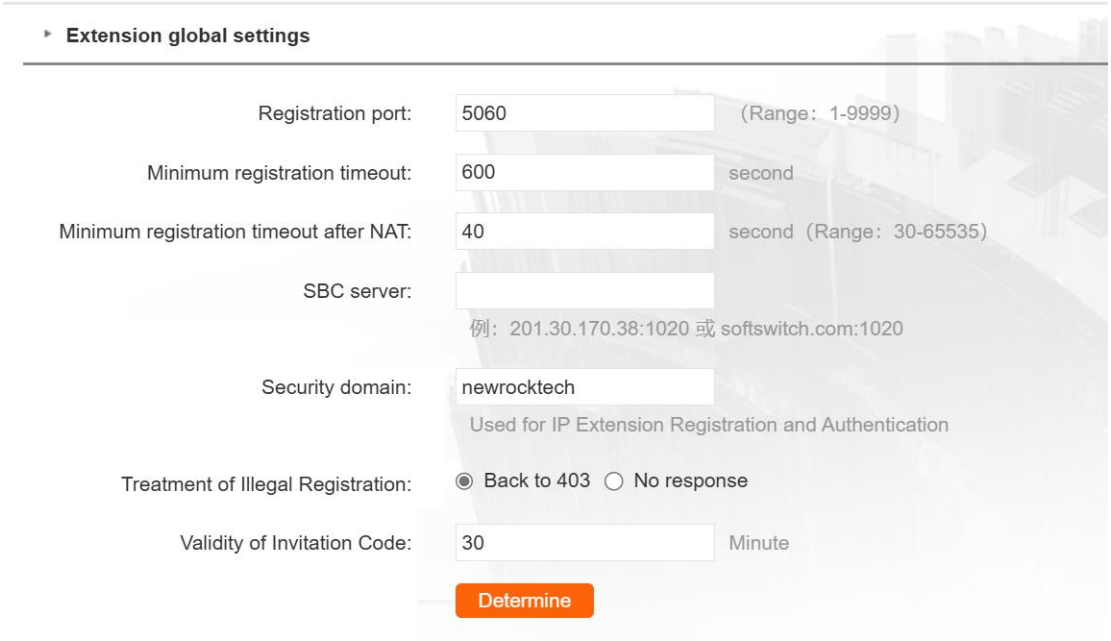


Table3.16 IP Extension Parameter Description

Item	Description
Registration port	Default 8090, cannot be the same as RTP port, SSH port.
SBC server	For remote IP extension authentication

3.3.2 Number Filtering

Click Extension settings>Number filtering to set the inbound/outbound number filtering rules applicable to all extensions.

For example, if 12345678 is set in Rejected Call Number, the device will play a busy tone alert when an incoming call comes from this number.

 Copyright © Redstone Systems, Inc

Figure3-6 Number Filtering Configuration Interface

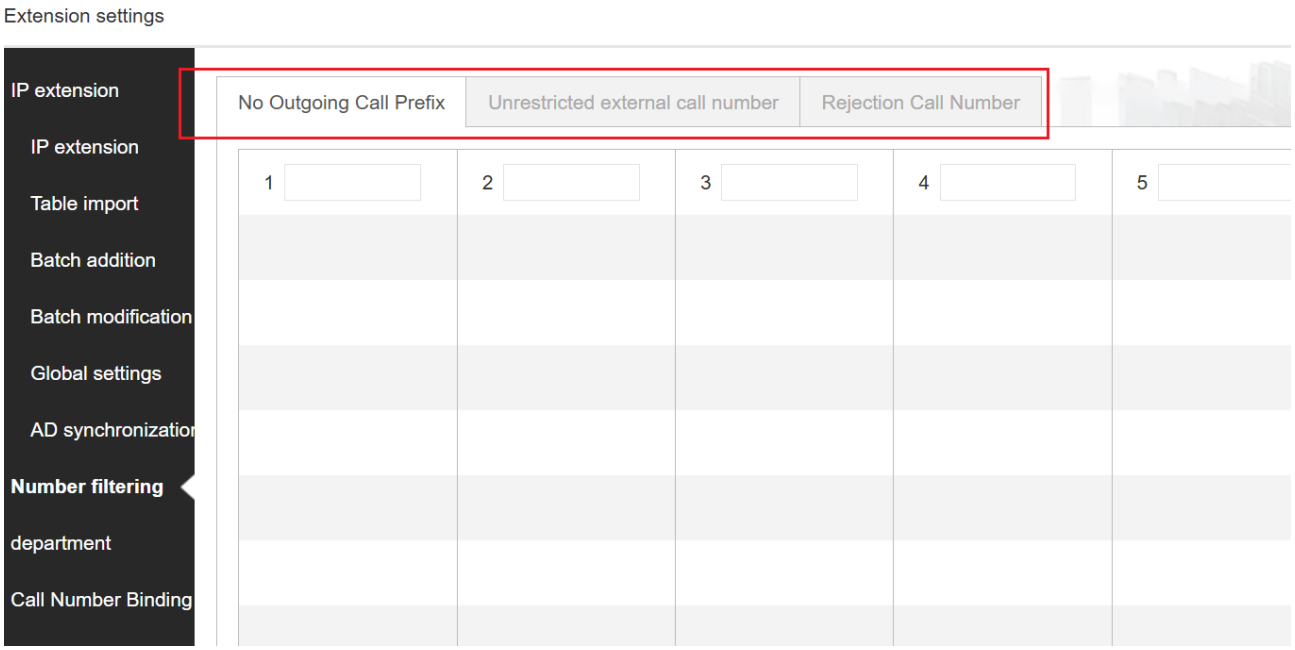


Table3.17 Parameter Description of Number Filtering Interface

Item	Description
No Outgoing Call Prefix	Extension users are prohibited from dialing numbers with no outgoing call prefix, and the device will play a busy tone alert when an extension user dials these numbers. Up to 20 prefixes or numbers can be set, separated by commas ",". Note: Numbers in the Unrestricted external call number are not subject to this restriction.
Unrestricted external call number	Unrestricted outbound numbers are numbers that all extensions can outbound call, even if the extension is configured with outbound permissions and prohibited outbound prefixes.
Rejection Call Number	When an incoming call from a rejected caller number comes in, the device will play a busy tone alert to reject this incoming call. Up to 30 rejected call numbers can be set. Note 1: This function requires an outside line to enable caller ID service. Note 2: Outbound calls are not affected by this table. Note 3: The reject call number configured here applies to all extensions, while the reject call number in the extension settings applies only to the corresponding extension.

3.3.2 Department

Extension users within the same department can use the Group Pickup feature to pick up each other's calls. To realize this feature, you need to configure the department and its affiliated extensions.

Step1. Click Extension settings>department to fill in or change the department name.

 Copyright © Redstone Systems, Inc

Click on the right side of the ⊕, more departments can be added.

Step2. Click Save.

Figure3-7 Department Configuration Screen

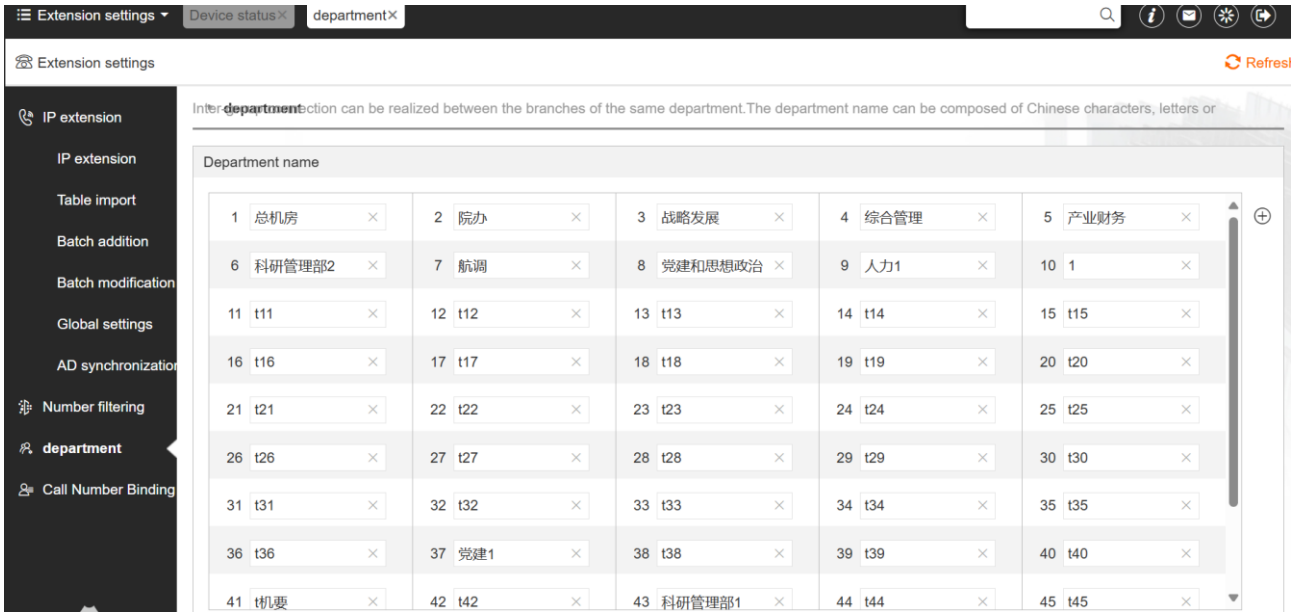


Table3.18 Parameter Description of Sectoral

Item	Description
Department	Extension users within the same department can use the Group Pickup feature to pick up each other's calls. To realize this feature, you need to configure the department and its affiliated extensions. Assigns extensions to departmental operations: 1.Go to Extension settings>IP Extension>IP Extension and click the button. 2.Select the department to which the current extension is categorized in the Department drop-down list and click OK to save the settings.

 Copyright © Redstone Systems, Inc

3.3.3 Call Number Binding Table

After binding an external caller's number to an extension, when that number subsequently dials the switchboard, the device will bypass the welcome message and go directly to the bound extension.

How to bind:

- After the extension hangs up, then take off the phone to dial *66, after hearing the voice prompts, that is bound to the caller number of the previous call

How to unbind:

- After the extension hangs up, then take off the phone and dial *67, and when you hear the voice prompt, you unbind to the caller ID of the previous call.
- View and unbind in the Extension settings>Call Number Binding Table in the device interface.

Figure3-8 Incoming Call Binding Table Screen

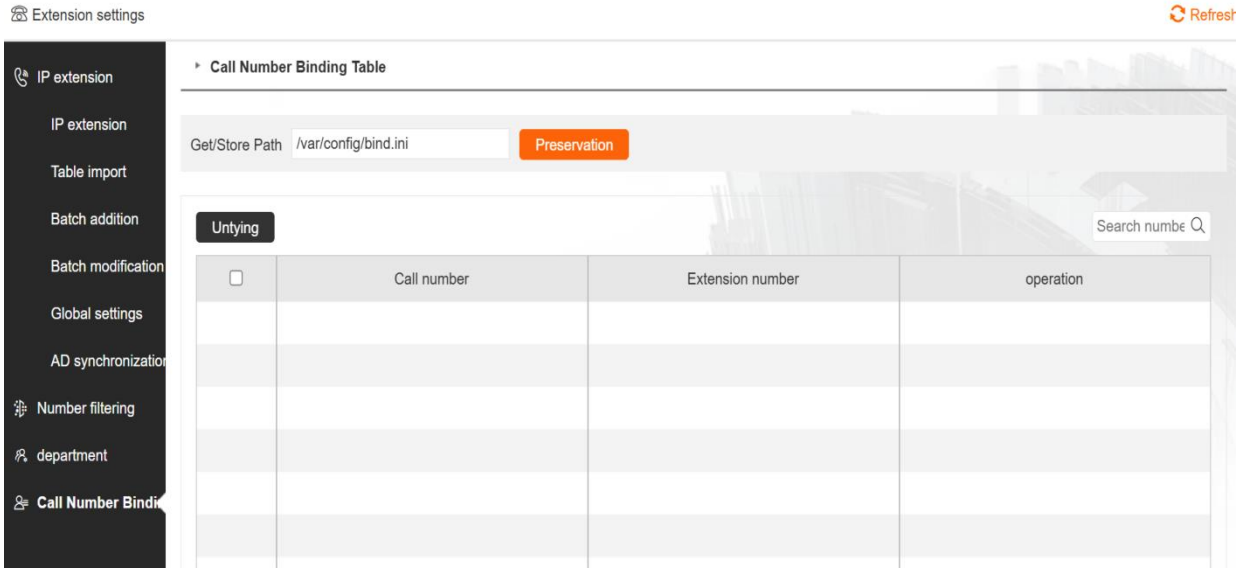


Table3.19 Parameter Description of Caller Binding Number Form

Item	Description
Get/Store Path	The path where the device stores the binding relationship. Modifiable.
Batch Unbundling	Batch unbinding of numbers.
Search Number	Enter the number to search. Fuzzy queries are supported.
Call number	Displays the phone number tied to the extension. Note: The interface only displays, you cannot change the number.
Extension Number	Displays the extension number to which the caller ID is bound. Note: The interface is only displayed and the extension cannot be modified.

 Copyright © Redstone Systems, Inc

Item	Description
Untying	Individual unbinding of numbers.

3.4 External line setup

3.4.1 SIP Outbound

SIP Outbound List

You need to apply for an account with your VoIP operator before you can set up a SIP outbound line. The account is then configured on the REX8000.

The configuration steps are as follows:

Step1. Click Outside Line Settings>SIP Outside Line>SIP Outside Line.

Step2. Click Add to fill in the registration information for the SIP outbound line.

Note: If the device needs to register to more than one SIP server, you need to turn on Register Multiple Platforms in the Outside Settings>Registration Options first.

Figure3-9 SIP Outbound New Interface

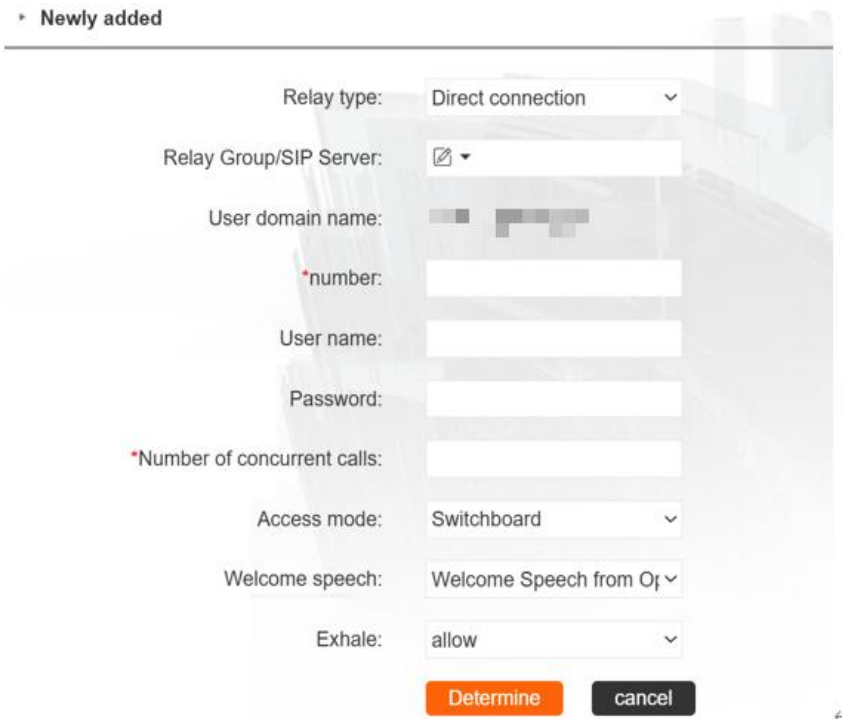


Table3.20 Description of SIP outbound registration parameters

Account Type	Item	Instructions
IP External Line	Relay Type	There are three types: Direct connection: point-to-point docking. Both parties are authenticated by the filled-in IP address. Registration: the REX registers to the SIP server. Registered: Remote The FXO port gateway is registered as a SIP outbound for the REX. The FXO port of the REX can be expanded. A registration user name and password must be set on the OM, and the gateway uses this user name and password to register to the REX.
	SIP Server	Fill in the server address and port provided by the VoIP operator. Note: When using a domain name address, you must also configure a domain name resolution server in the "Basic Setup > Network Configuration" interface.
	Relay Group	See.3.4.2 Direct relay group
	User domain name	Provided by VoIP carriers such as salesdepart.abccompany.com.
	Numbers	The trunk type is the outgoing number provided by the VoIP operator when registering, e.g. 62019550185. Note: All outside numbers cannot be duplicated, nor can outside numbers be duplicated with extension numbers. A number is created here for the FXO port gateway to register to the OM when the trunk type is Registered.
	User name	Fill in according to the requirements of the VoIP operator for the registration and authentication of the SIP outside line. If not filled in then use the number to authenticate.
	Password	Provided by the VoIP service provider.
	Number of concurrent calls	The maximum number of simultaneous calls that can be made through this outside number. Note: The number of concurrent calls to a single outside number cannot exceed 200 (measured), and the sum of the number of concurrent calls to all outside numbers cannot exceed the maximum number of SIP outside numbers of the device.
	Access mode	Select the access method for this outside line: • Switchboard: Incoming calls to this outside line are handled using the automatic switchboard method. • Straight Line: Binds an outside line to an extension, and when an incoming call comes in, the device bypasses the automated switchboard and delivers the call directly to the bound extension.

 Copyright © Redstone Systems, Inc

Account Type	Item	Instructions
	Welcome speech	Select the voice navigation played by this outside line for incoming calls. This item can be configured only when you select the access mode as the switchboard. • Switchboard Welcome Message: Indicates the use of voice navigation configured using the Basic Setup>Switchboard page. This is the default option. • IVR: Select a multi-level IVR for voice navigation. • Voice: Select a single voice file for voice navigation. Note that the voice file selected here will only be played during working hours, and only voice navigation configured on the Basic Setup>Switchboard page will be played during non-working hours. Note: The device has an upper limit of up to 30 simultaneous voice files allowed to be played, so the device can play a welcome message for up to 30 inbound lines at the same time.
	Direct Inward Dialing (DID)	Fill in the extension or extension group number tied to this outside line. Note: This needs to be configured when you select the access mode as straight line. There are three ways: 1.Select the same extension number 2.Call Pickup Group Number 3.X digits after the outside number, plus the prefix B for the line number of the outside line. For example, the outside number is 1234, X=3, B=9, and the final configured straight line number is 9234.
	Exhale	When the access method for an outside line is set to switchboard, there are two types of outgoing privileges for that line: • Allow: Allows outgoing calls over the line, i.e. the line can be used for both incoming and outgoing calls. • Forbidden: outgoing calls over this line are forbidden, i.e. the line is only used for incoming calls. When the access method of an outside line is set to straight line, there are two types of outgoing privileges for that line: • Shared: this outside line can be shared by other extensions. • DID Dedicated: this outside line is reserved for the exclusive use of a bonded extension or group of extensions.

Step3. Click OK to return to the SIP Outside Line Configuration screen to view the registration status of the configured SIP outside line.

 Copyright © Redstone Systems, Inc

Figure3-10 SIP External Line Configuration Interface

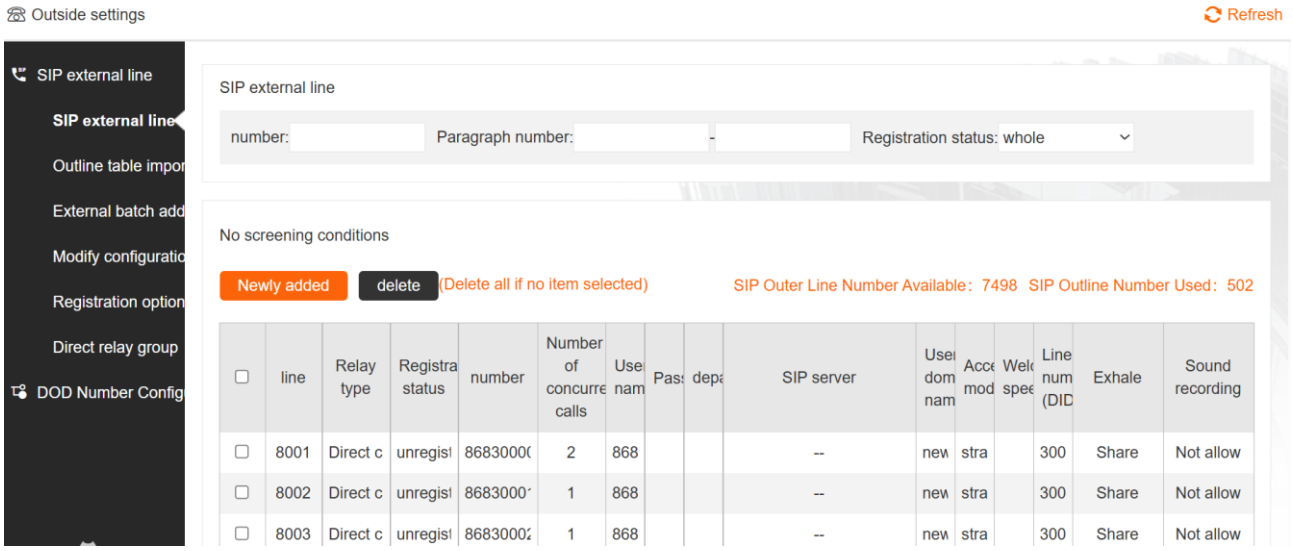
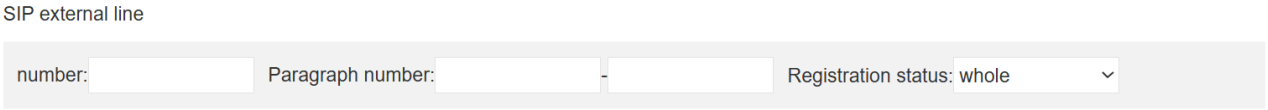


Table3.21 SIP External Line Interface Parameter Description

Item	Description
Registration Status	There are 5 registration statuses: • Successful registration: Indicates that this SIP outside line is available for use. • Registration Failure: Indicates that there was an error in the registration of the SIP outside line. At this time, this SIP external line cannot be used, and the problem can be analyzed according to the returned error code. • Unregistered: registration option is unchecked. • Timeout: Indicating that the registration was not successful within the registration time limit. This SIP external line is not available at this time. Please check if this SIP outbound account is already in use. • Registration in progress: Indicates that the SIP outside line is being registered.
Sound Recordings	Turn on the recording function for the outside line. Note: To enable recording, you also need to enable the recording function in the Application Services>Recording page. For details, see 3.5.3 .
Delete	Check the box to delete the specified SIP outside line. If you do not check the box, click Delete directly, which represents the full selection of deletion

Query: You can input the outside line number, range, select the registration status and then click the query button to query the specific information of the extension. Also click

on More Filtering Select more filtering criteria.



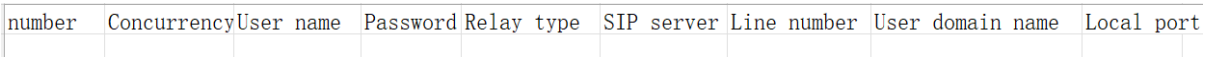
Outside table import

For easy configuration, REX8000 supports batch import of multiple SIP outside accounts via Excel (up to 1000 SIP outside accounts at one time).

Step1. Click Outside settings>SIP external line>Outside table import.

Step2. Click on the Template download.

Step3. Open the downloaded template sip_import_template.xlsx and fill in the outside line information in the format. Save.



number	Concurrency	User name	Password	Relay type	SIP server	Line number	User domain name	Local port

Step4. Click Excel template import and select the prepared template to import.

When the import is complete, the imported numbers are displayed in the table below.

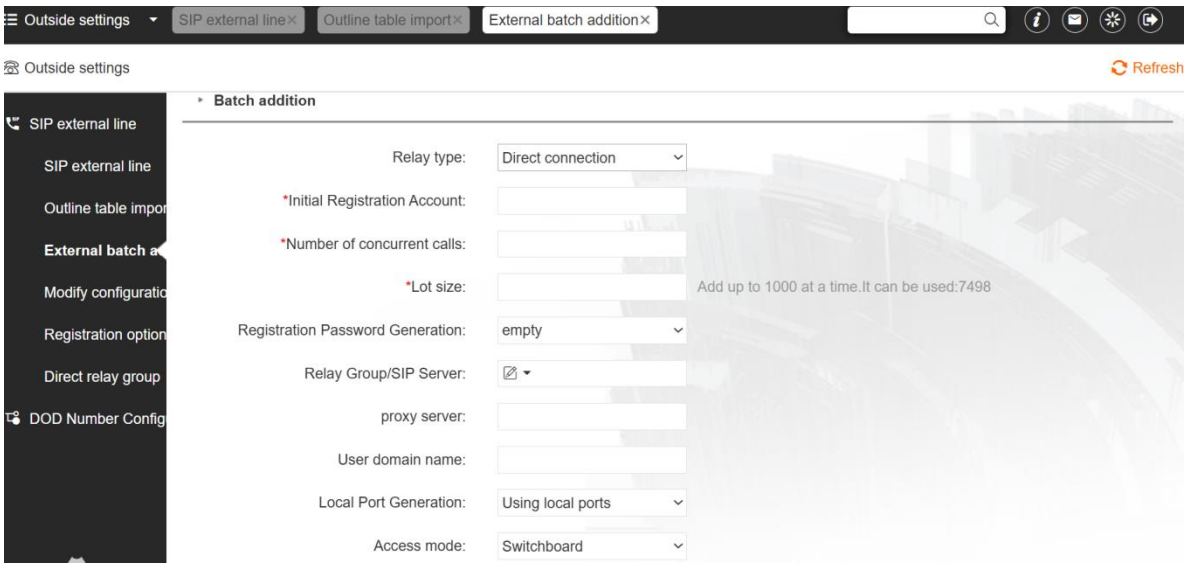


External Batch Addition

To simplify the configuration, REX8000 supports batch adding SIP outside line accounts, and all SIP outside lines added in a batch have the same function enabled. If different functionality is required, it will need to be modified again separately. Supports batch adding up to 1000 SIP outside lines at a time.

Click Outside settings > SIP external line> External batch addition, enter the starting registered account and batch number of the SIP Outbound, fill in the number of concurrent calls, etc., and click OK.

 Copyright © Redstone Systems, Inc

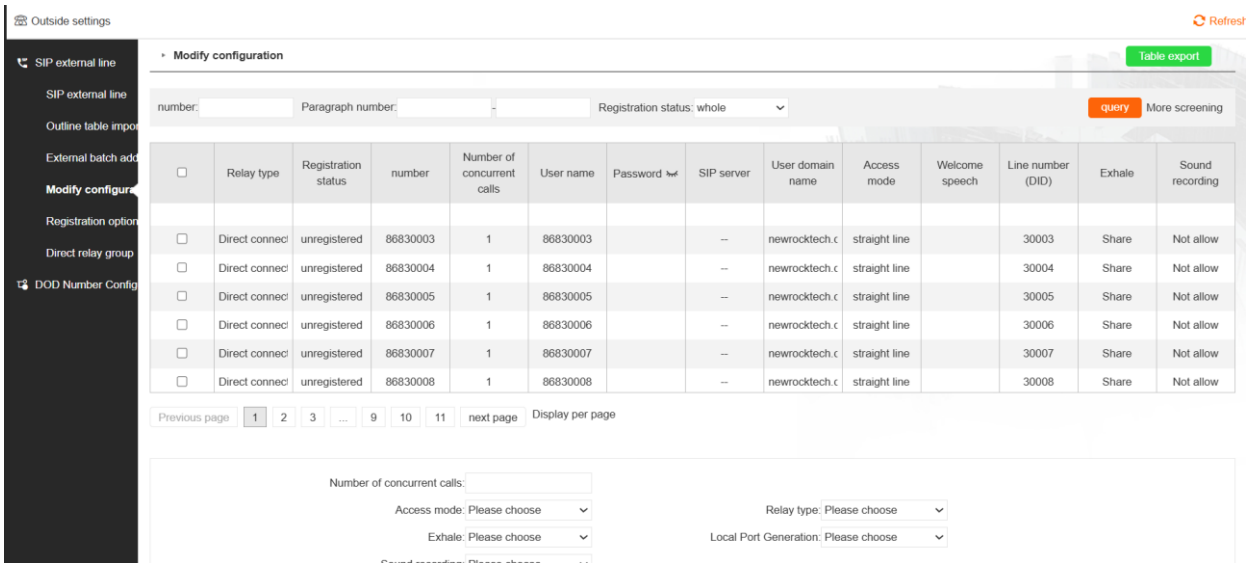


Outside line Batch modification

For easy modification, REX8000 supports batch modification of external line configuration.

Click Outbound settings > SIP external line> Modify configuration to filter out the outbound numbers you want to modify, and then check these numbers and modify the configuration uniformly at the configuration below. Click OK after making the changes.

Filter out the desired outside line numbers, and then check the outside lines that need to be modified and modify the configuration. Click OK after the modification.



Registration Options

Click Outbound settings>SIP external line>Registration options to modify the local port, registration timeout and other information. It is recommended to change the default local port to avoid SIP attacks.

Figure3-11 SIP Outbound Registration Options Screen

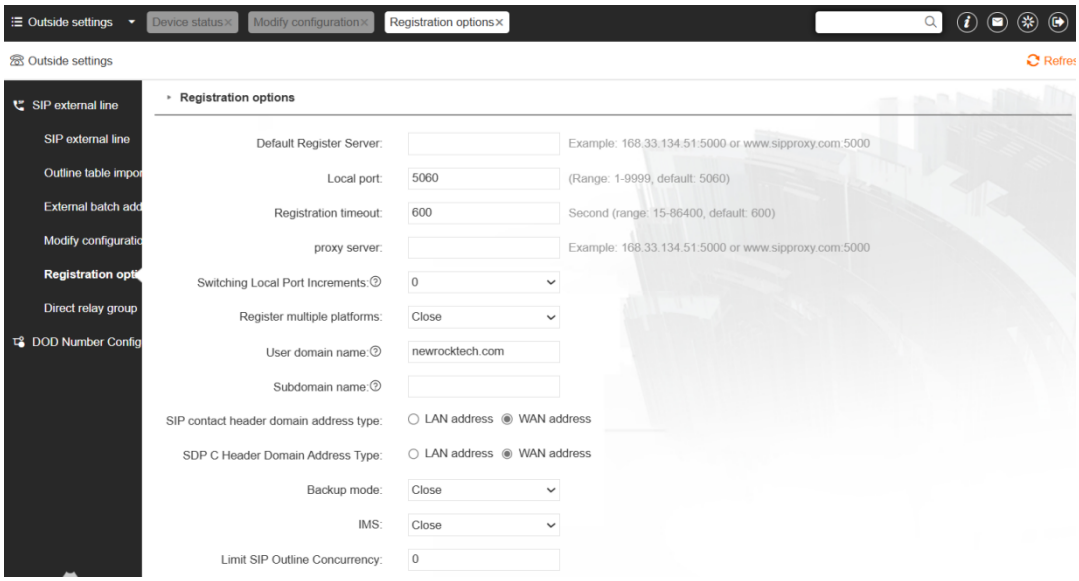


Table3.22 Parameter Description of SIP Outbound Registration Options

Item	Description
Default Registration Server	Configure the address and port number of the SIP registration server, the address and port number should be separated by ":". No default value. The registration server address can be in the form of an IP address or in the form of a domain name. For example, 168.33.134.51:5000 or www.sipproxy.com:5000. When using the domain name form, you need to enable DNS service and configure DNS server parameters in the Basic setup > Network Configuration interface. The configuration of this parameter is automatically invoked when the SIP server address of a single line is not filled in.
Local port	The port on which the device sends SIP messages to the registration server, i.e., the local SIP port, defaults to 5060 and can be changed. It is recommended to modify this port value to avoid SIP attacks.
Registration Timeout	The period for the device to register with the server, range: 15~86400, default: 600. Fill in according to the operator's requirements.
Proxy Server	It is usually sufficient to keep in line with the registration

 Copyright © Redstone Systems, Inc

Item	Description
	server. If the operator provides a separate proxy server, fill in the form as required by the operator. When using domain name, you can enable the backup mode and fill in a backup IP address to the "backup server", which is used for the device to switch to this IP address when the domain name resolution service fails.
Switching Local Port Incremental	Configure the local port transformable range. After a failed call or registration, the local port automatically adds 1 to try again, and when the incremental value reaches the configured value, a new cycle begins. The default value is 5.
Register multiple platforms	Enabled to allow multi-platform functionality, i.e., to allow the configuration of different registration servers and client-side domain names for each IP outside line.
User domain name	The attribution of the IP outbound number, provided by the SIP outbound carrier, example: abccompany.com.
Subdomain name	The attribution of the IP outbound number, provided by the SIP outbound operator, is used in conjunction with the SIP client-side domain name. If the domain name is configured as abccompany.com and the subdomain is configured as ims, the complete domain name is ims. abccompany.com.
SIP contact header domain address type	Set the content of the IP address carried in the SIP Contact header field. If the device is in the intranet (after NAT) and encounters the problem of voice single pass during outbound call, you can try to adjust this parameter to solve the single pass problem. • LAN address: Use the LAN address configured by the device itself. • WAN address: Use the detected NAT-transformed public network address.
SDP *C* Header Domain Address Type	Set the content of the IP address carried by the Connet under SDP in the call. If the device is in the intranet (after NAT) and you encounter the problem of voice single-passing during outbound calls, you can try to adjust this parameter to solve the single-passing problem. It is recommended that this parameter be set to the same value as Contact. • LAN address: Use the LAN address configured by the device itself. • WAN address: Use the detected NAT-transformed public network address.
Backup mode	• Off: Disables backup server configuration, i.e., backup server registration is not enabled when the primary server is unavailable. • Fixed: Backup server configuration is on and the server address is pre-set in the backup server. The backup server address is provided by the VoIP operator.

 Copyright © Redstone Systems, Inc

Item	Description
	• DNS SRV: Backup server configuration is on, and the device obtains multiple IP addresses through domain name resolution, the first address is the primary server and the second is the backup server.
Backup Server	Backup SIP servers can be set up. After successful setup, the backup server will be enabled automatically when the main SIP outbound server is unavailable. Note: The primary server address is configured in the "Proxy Server" section. Other SIP servers configured for SIP extranets after the multiplatform is turned on do not support the backup mechanism.
SRV Refresh Interval	• Use the time parameter (TTL) carried in DNS messages:default configuration. • Custom: customize the refresh interval, the value range is 1~65535 seconds.
Local Port	The port on which the device sends DNS query requests. The default is 1026.
Server Port	The receiving port of the DNS server. The default is 53.
Number Of Timeout Retransmissions	The number of retransmissions of DNS SRV query requests sent by the device to the DNS server when the DNS server does not respond. The default is 3.
Master Server Cutback Interval	When using a standby server, you can set up a timed registration request to the primary server to cut back to the primary server. This sets the time interval for sending this request, the default is 300 seconds.
Send NAPTR Query Before SRV Query	Configure to send NAPTR queries before SRV queries.
Class A Query Send Condition After Srv Record Return	Configure the conditions for sending a Class A query after an SRV query request returns: • Always send: Class A query request is sent regardless of the type of data returned by the SRV query request; • Sent only when the SRV returns a result as a domain name: Class A query request is sent only when the SRV query request returns data as a domain name. The default is this item.
DNS Server	Used only for resolving SIP servers.
IMS	Check the box to turn on IMS.
To Show How To Get The Information.	When a call is received on an IP outside line, the incoming display can choose to get it from the P-Asserted-Identity header field of the SIP message or from the From header field.
Access Network Information	Include the IP address and port number of the access network, e.g., 192.168.100.200:5060. Not required, fill in as required by your IMS service provider.

 Copyright © Redstone Systems, Inc

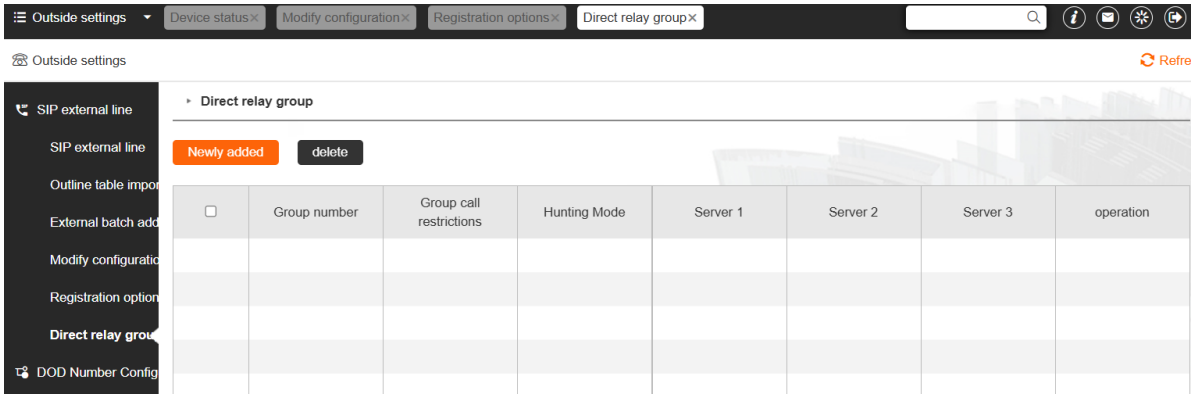
Item	Description
Limit SIP Outsline concurrency	The check box allows you to configure the upper limit of the total number of concurrent calls to all SIP outside lines. The upper limit cannot exceed the total number of SIP outside lines.

3.4.2 Direct Relay Group

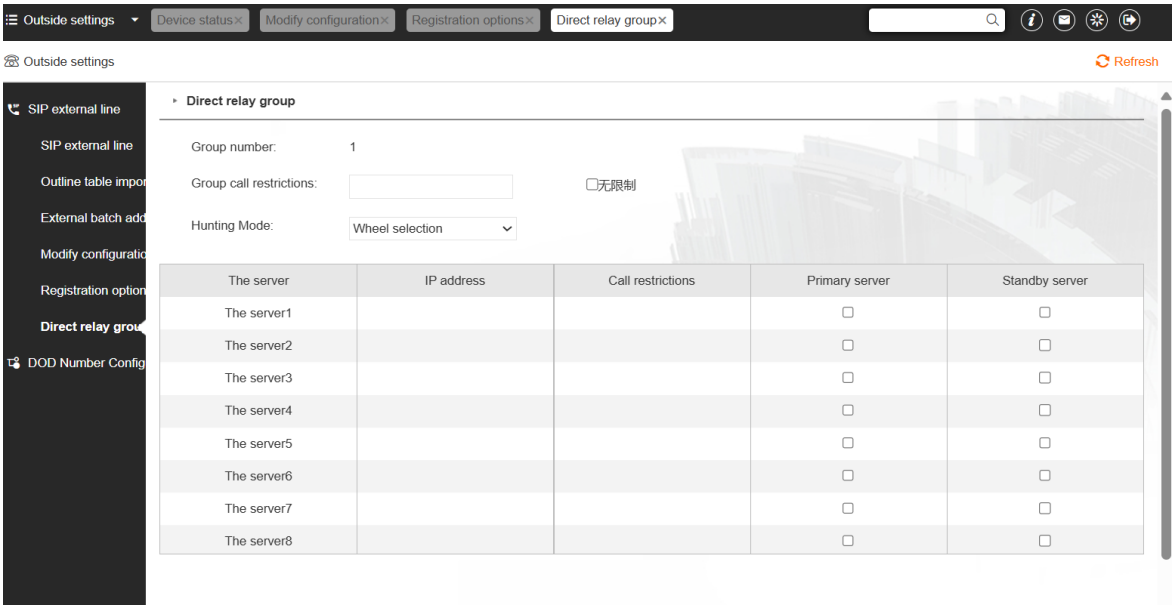
This function is used in conjunction with the RedStone REX Trunk Gateway. After the configuration is completed, all SIP outbound calls will be outbound from the REX.

Step1. Click Outside settings>SIP external line>Direct relay Group.

Step2. Click Add and fill in the two server addresses (i.e., the addresses of the two REX, which will automatically switch to the other if one has connection problems).



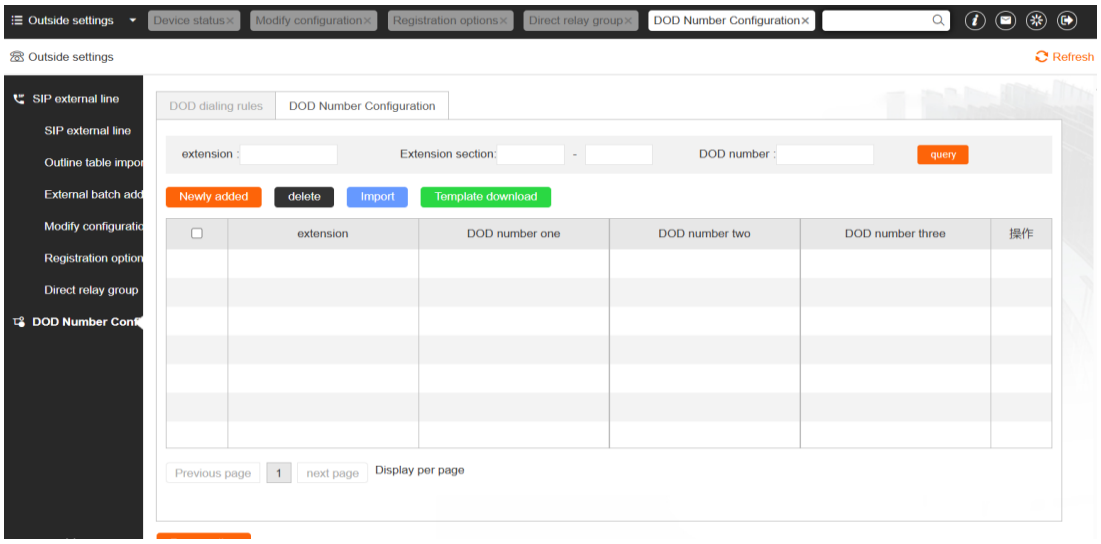
Step3. Click Outside settings>SIP external line, set the trunk type of the outside line toDirect Connection, and select the trunk group configured in the previous step for the trunk group/server.



3.4.3 DOD Number

DOD (Direct Outward Dialing), i.e., extension direct outward dialing, is used in the case where an extension number is bound to multiple outgoing numbers, and the function is divided into two parts: DOD dialing rules and DOD number configuration.

Step1. Click SIP Outbound>DOD Number Configuration.



Step2. Configure the binding relationship between extension numbers and outside numbers.

An extension number can be tied to a maximum of three outside numbers.

If you need to configure bound outside numbers for a large number of extensions, we recommend you to click "Template Download", then edit the template and click "Import".

A screenshot inside the template dod_import_template.xlsx is shown below:

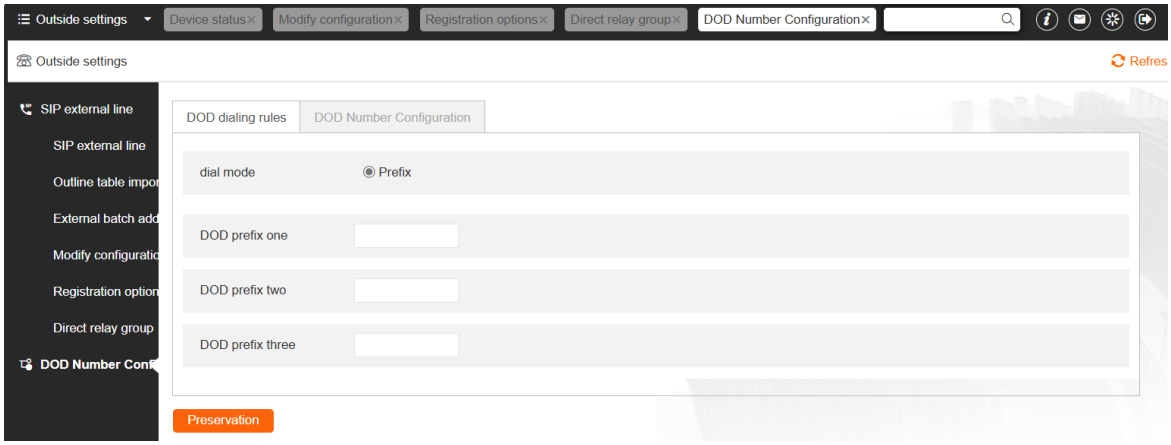
Extension	DOD number 1	DOD number 2	DOD number 3

Step3. Configure DOD dialing rules.

When an extension number is bound to three outside numbers, and that extension makes an outgoing call, you need to dial the prefix corresponding to the outside line to select the outside line used for the outgoing call.

 Copyright © Redstone Systems, Inc

Figure3-12 Linear (DID/DOD) Configuration Interface



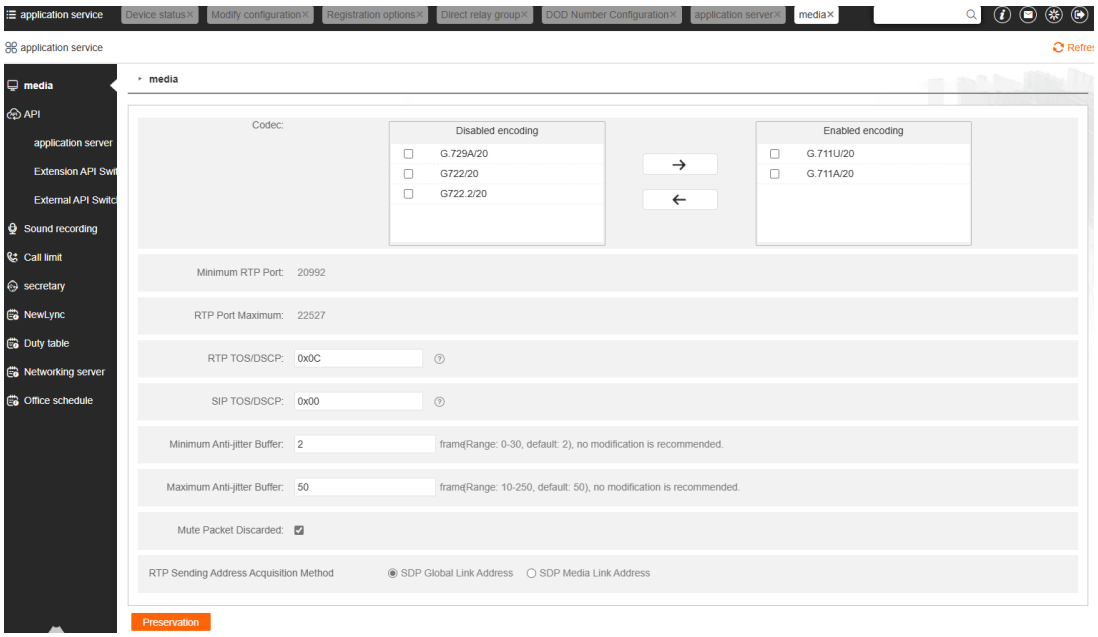
Item	Description
DOD Prefix	The three prefixes of DOD dialing rules correspond to the three external lines configured on the Number Configuration page.

3.5 Application Service

3.5.1 Media, Esp. News Media

Go to Application services>media to configure Voice over IP media parameters.

Figure3-13 Media Configuration Interface



 Copyright © Redstone Systems, Inc

Table3.23 Description of media parameters

Item	Description
Codecs	The device supports multiple codecs: G.729A/20,G.711U/20,G.711A/20,G.722.2/20,G.722/20. When multiple encoding methods are enabled, the device will negotiate codecs with the peer SIP device in front-to-back order.
RTP Port Min.	Minimum value for RTP transmit and receive ports.
RTP Port Maximum	The maximum value of the RTP transmit and receive ports.
RTP TOS/DSCP	Defines the service level QA for different priority levels, the default value is 0x0c. This parameter needs to be used in conjunction with the router's QoS feature to ensure the voice quality of IP calls.
Min. Anti-jitter Buffer	The RTP Jitter Buffer helps to overcome the effects of network jitter. This parameter configures the minimum number of RTP packets that can be retained in the buffer, the default value is 2 frames. The range of values is 0 to 30 frames.
Max Anti-jitter Buffer	The RTP Jitter Buffer helps to overcome the effects of network transmit jitter. This parameter configures the maximum number of RTP packets to be retained in the buffer, the default value is 50 frames. The range of values is from 10 to 250 frames.
Mute Packet Discarded	Checked indicates that received RTP SID voice data frames are discarded. The default value is unchecked. Note: This parameter needs to be configured only if the received SID data frame does not meet the specification. For example, the device receives certain unregulated RTP SID data with varying data lengths, which can cause the caller to hear a murmur or certain strange sounds.
RTP Sending Address Acquisition Method	• SDP Global Link Address (default): obtains the peer IP address from the SDP global connection; • SDP Media Link Address: Get the IP address of the opposite end from the Connection Information after the SDP Media Description (Media Description).

3.5.2 API

API is the application programming interface provided by the device. External applications can perform operations such as call control, call status monitoring, and configuration placement on the device through the API, and the device can push reports such as events and call logs to the application through the API.

To use the API, the following configuration steps need to be performed on the device:

Step1. Go to application service > API and fill in the API server address (i.e. the address

of the external application).

Figure3-14 API Configuration Interface

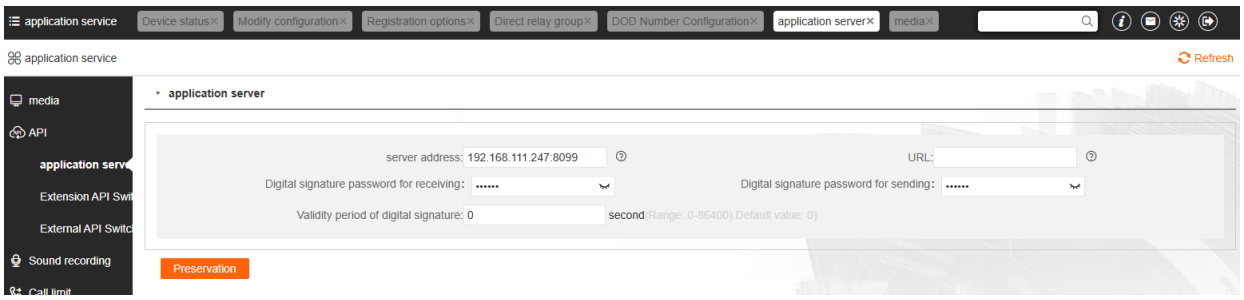


Table3.24 API Interface Parameter Description

Item	Description
server address	After selecting Customize, enter the third-party application server address and port number. The default value of 80 is used when the port number is not specified. The REX only recognizes API request messages from this IP address, and when the REX needs to proactively push API report messages to the application server, it also pushes to this address.
URL	Enter the address (relative path) of the Web page used by the application server to receive device messages.
Digitally signature password for receiving	The REX only receives API request messages from authenticated application servers. After configuring the REX digital signature authentication password, the key assigned on the application server needs to be consistent with the one configured here.
Digitally signature password for sending	The REX can send API requests to the application server only after it has been authenticated by the application server. The digital authentication password configured here needs to be the same as the key configured on the application server.
Validity period of digital signature	Configured when digital signature authentication is used. The range of values is from 0 to 86400 seconds, and the default is 0 for permanent effect.

Step2. Turn on the Extension API on the Extension API Switch page and turn on the Outside API on the Outside API Switch page.

Step3. Save the configuration and reboot the device.

Note

When the device receives the message, it prioritizes the authentication of the application server through the configured server address, and then performs digital authentication if the authentication fails.

 Copyright © Redstone Systems, Inc

Extension API Switch

The Extension API switch is used to control whether an extension actively reports status to the API server.

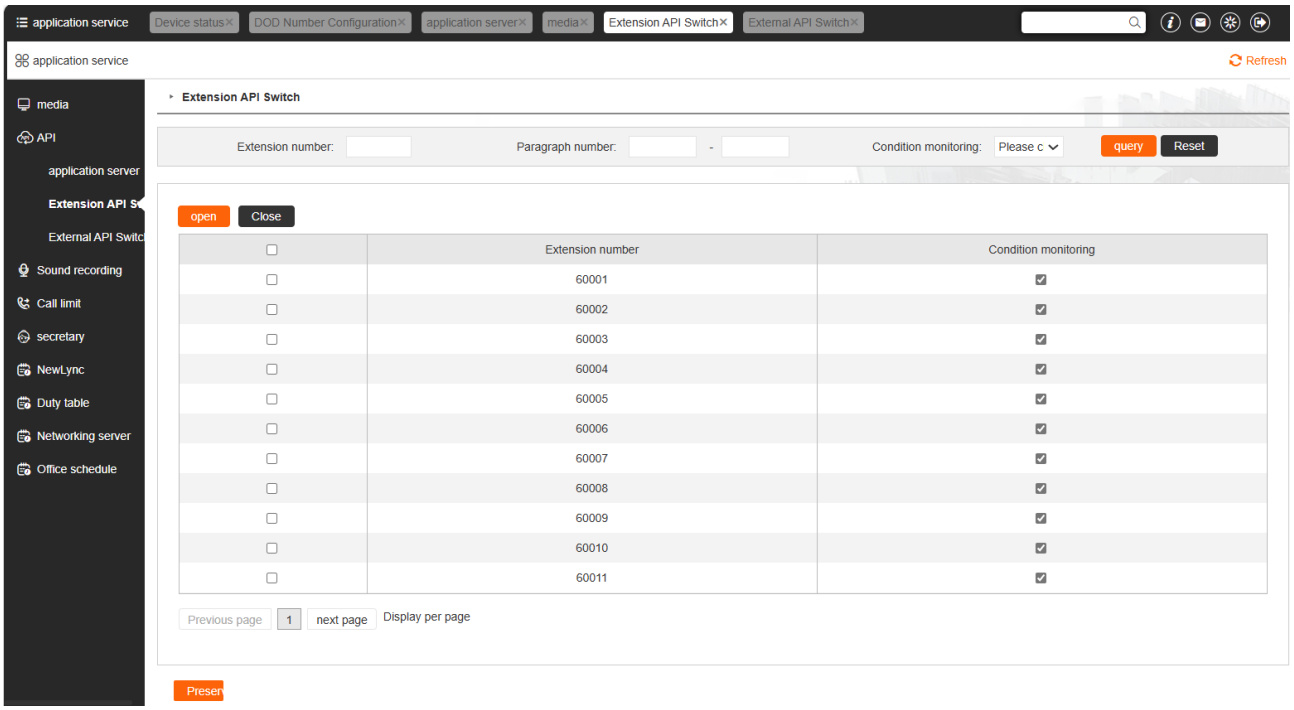


Table3.25 Extension API Switch Parameter Description

Item	instructions
Extension number	Enter the extension number and click Query to search by extension number in order to locate the extension that needs to be configured with the API as soon as possible.
Numbering Section	Enter the starting extension number and the ending extension number, and click Query to search by range of extension numbers in order to locate the extension segment for which the API needs to be configured as soon as possible.
Condition monitoring	Search Area: Used to filter by whether the extension has status monitoring turned on. Result display area: Checking indicates that the status monitoring function of this extension is enabled.
On/Off	Used for batch turn-on or turn-off status monitoring function for selected multiple extensions.

 Copyright © Redstone Systems, Inc

Outside API switch

The Outside Line API switch is used to control whether the application server can control outside lines through the API.

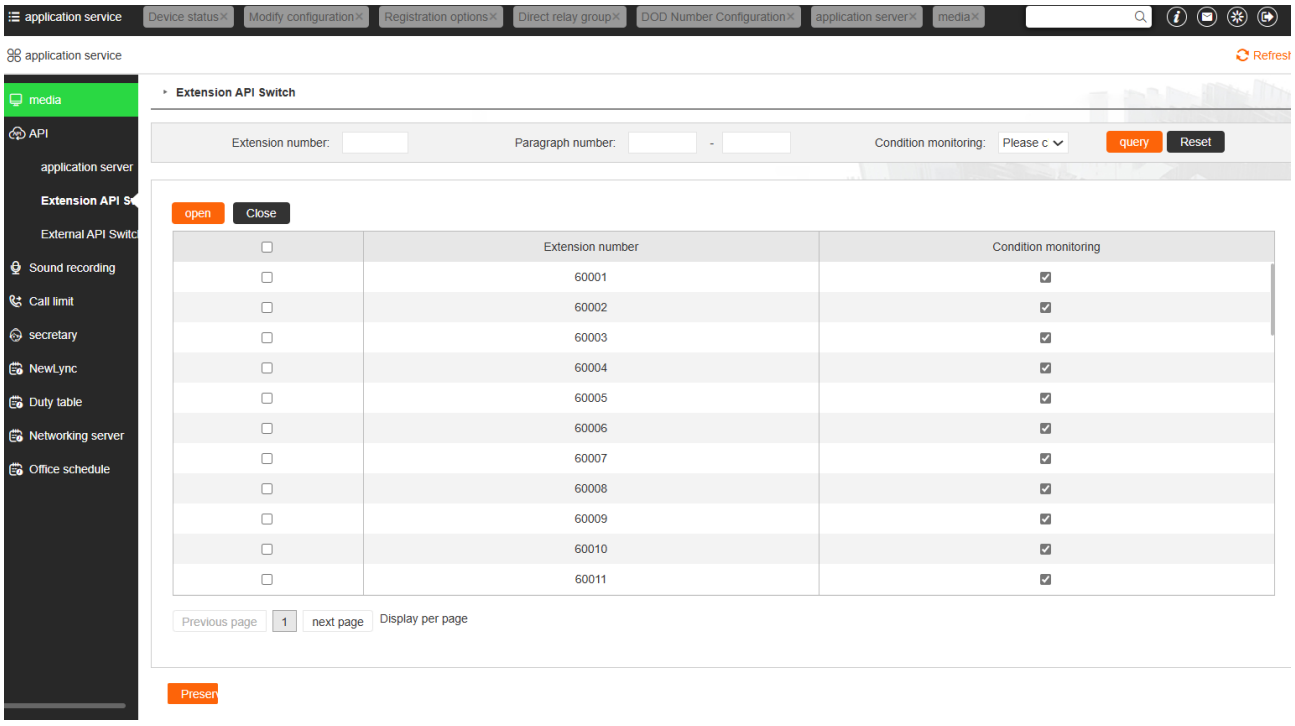


Table3.26 Outside API switch Parameter Description

Item	Instructions
Outsider Number	Enter the outside line number, click Search, and search by outside line number.
Numbering Section	Enter the Start Outside Number and End Outside Number and click Query to search by the range of outside numbers.
Condition Monitoring	Query Zone: Checked means only query the outgoing numbers that have this feature enabled. Result display area: when checked, it indicates that the application server can monitor the status of this external line.
Incoming Call Pre-Answer Control	Query Zone: Checked means only query the outgoing numbers that have this feature enabled. Result display area: when checked, it means that the application server can control the incoming callsfrom this outside line before answering.
Incoming Call Answering Post Control	Query Zone: Checked means only query the outgoing numbers that have this feature enabled. Result display area: checking indicates that the application server that opens this outside line can control the incoming calls from this outside line after answering.

 Copyright © Redstone Systems, Inc

Item	Instructions
On/Off	Used to batch turn on or off multiple selected outside lines.

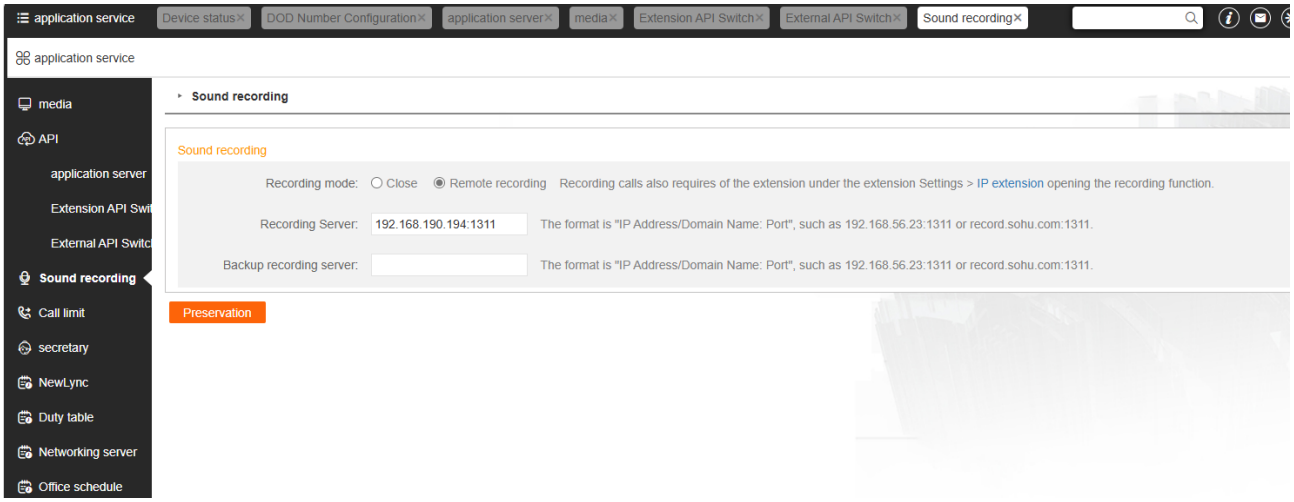
3.5.3 Sound Recordings

The remote recording method stores the recording files generated by the device in real time on a pre-deployed external recording server. The recording server is installed with the RedStone recording agent software or the RedStone recording management system.

The configuration steps are as follows:

Step1. Click application service>Sound recording and select Remote recording.

Figure3-15 Remote Recording Configuration Interface



Step2. Fill in the IP address and port number of the recording server (default is 1311), e.g. 192.168.10.1:1311.

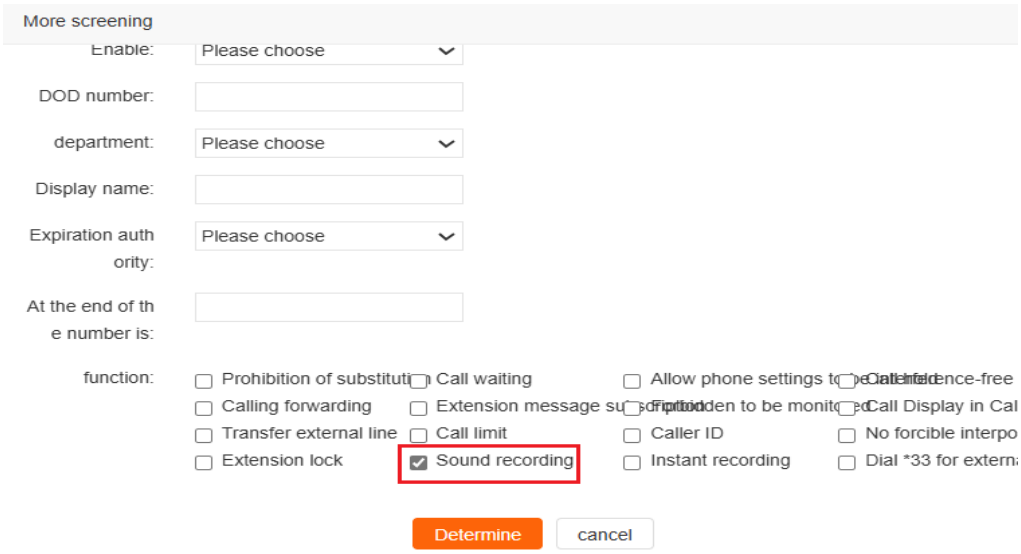
Step3. Save the settings.

Step4. Go to Extension Settings>IP Extension, select the extension that you need to enable the recording function, and click the button.

Step5. Check the Sound recording in the Extension function.

Figure3-16 Extension Recording Configuration Interface

 Copyright © Redstone Systems, Inc



Step6. Click OK.

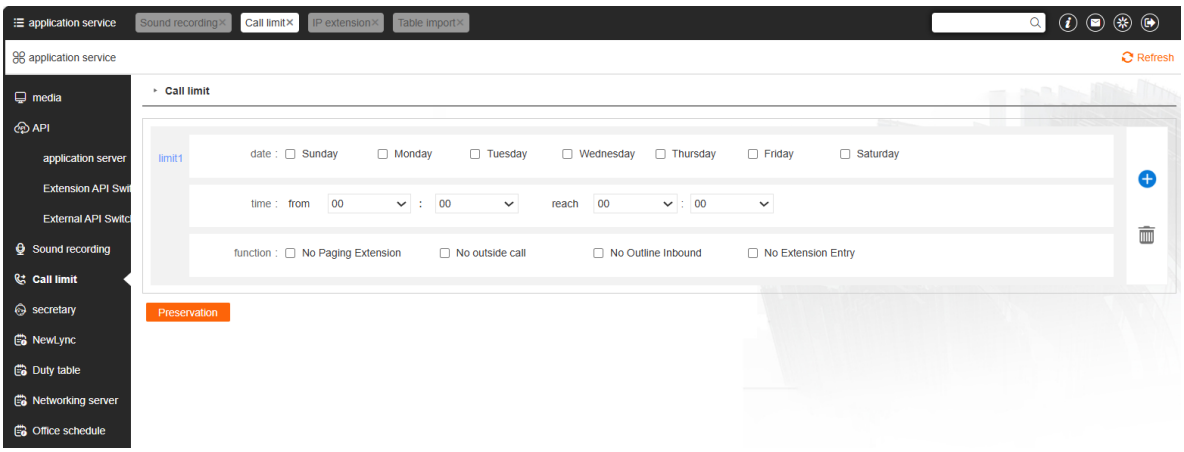
3.5.4 Call limit

The device can restrict the outbound and inbound functions of an extension by time periods according to preset time and function templates.

Step1. Go to application service>Call limit to set the time for the restriction to take effect and the extension inbound/outbound restrictions. For example, on Mondays, from 00:00 to 08:00, outgoing calls are prohibited.

Step2. Click Add to add call restrictions.

Figure3-17 Call barring configuration screen



Step3. Save the settings.

Step4. Go to Extension Settings>IP Extension, click the corresponding action icon of

 Copyright © Redstone Systems, Inc

the extension. Click on the icon corresponding to the extension, and check the call limit function of the extension.

Step5. Save the settings.

3.5.5 Secretary

By tying an extension to a secretarial extension, calls to that extension will be routed to the secretarial extension and answered by the secretary. The secretary function can be turned on/off with the handset function code *35.

Step1. Go to application services > secretary and click Add.

Step2. Select the extension number and the corresponding secretary extension for which a secretary needs to be configured.

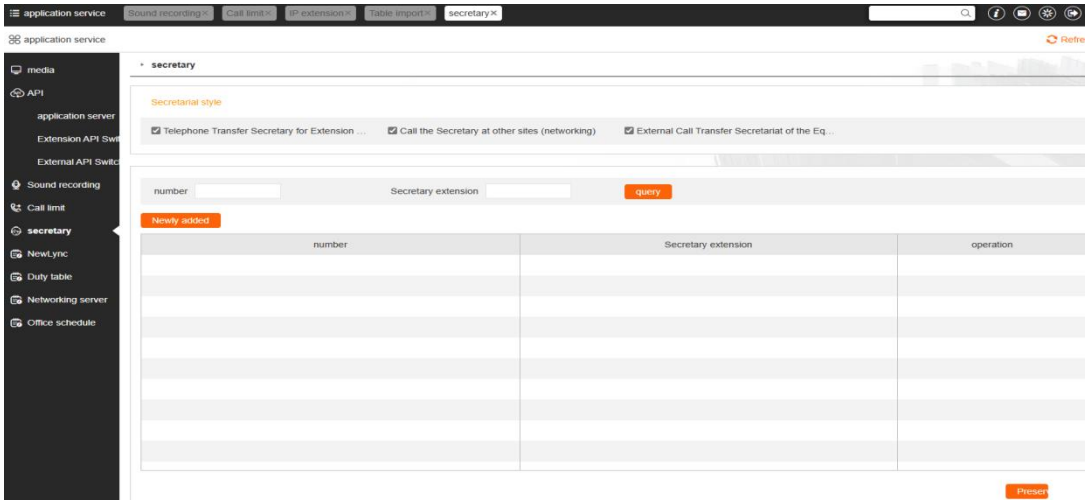


Table3.27 Secretary Parameter Description

Item	instructions
Secretarial approach	Outside calls from this device to Secretary: Forward outside calls from this device to the Secretary's phone.
	Incoming Calls from this facility's extension to Secretary: Forward calls from this device extension to the Secretary's phone.
	Incoming Calls from Other Sites to Secretary (Group Network): Forwards all calls (both extensions and outside lines) from other devices in a multi-point group network to the secretary's phone.

Step3. Click Save.

3.5.6 Duty Roster

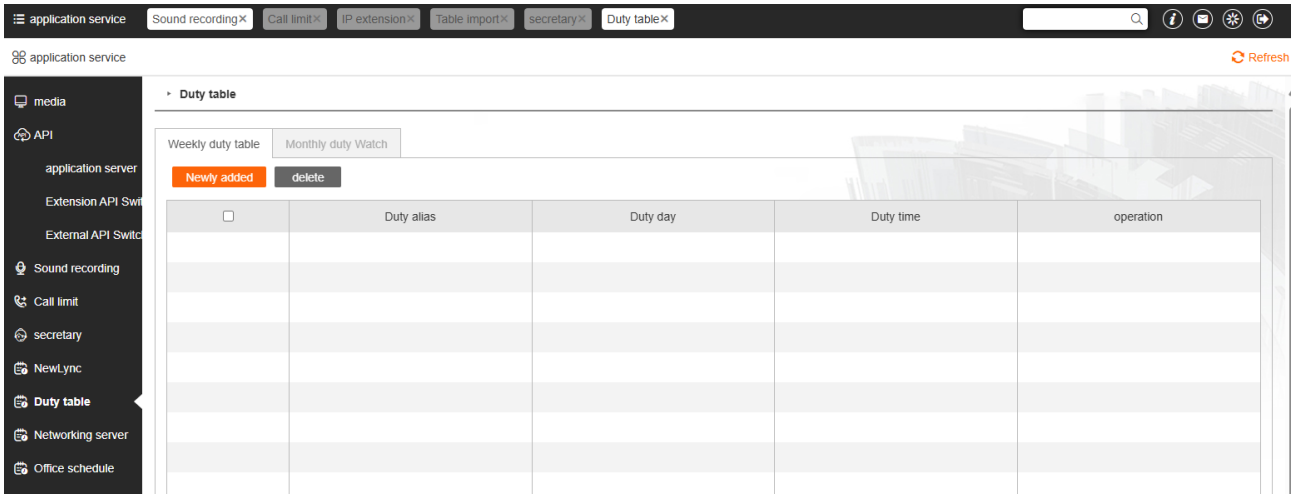
The Duty List is used to configure the duty officer who answers incoming calls from outside the facility during non-working hours. This function is divided into two ways: weekly duty and monthly duty.

Step1. Go toApplication Services>Duty List.

Step2. Select the mode of duty.

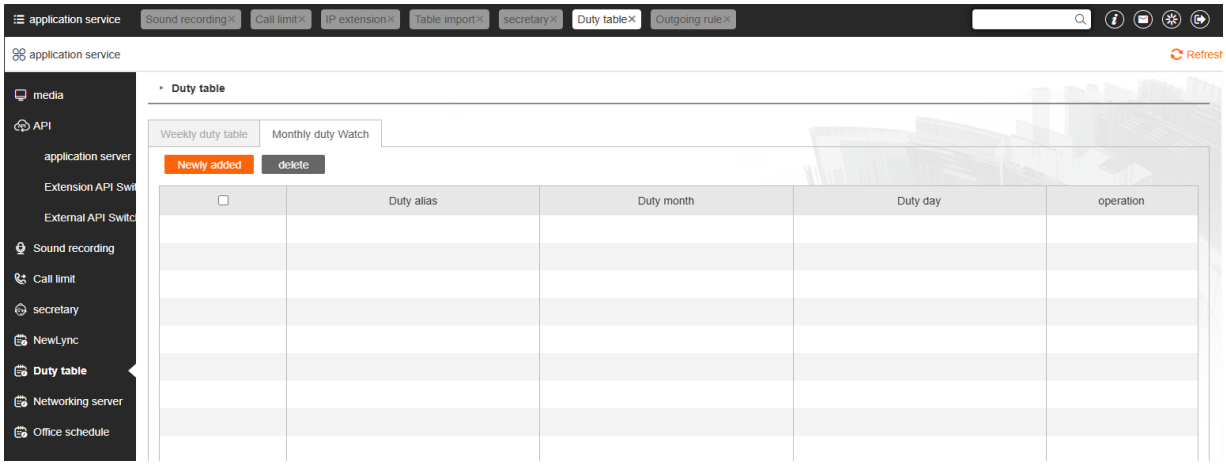
Weekly duty roster

After setting up the weekly duty schedule, the outgoing calls will be forwarded according to the set duty personnel every week, i.e. the cycle will be effective on a weekly basis. Up to 5 weekly duty rosters can be added with the following interface.



Monthly Duty Roster

When you set up a monthly duty list, it is used to specify the duty personnel for a specific month and is not valid for other months. Up to 5 monthly duty rosters can be added with the following interface.



Step3. Added duty roster.

Weekly Duty Roster

ClickAddto enter the Weekly Duty List Configuration screen, as shown below.

After completing the settings, clickSave. The weekly duty roster will recur on a "weekly" basis.

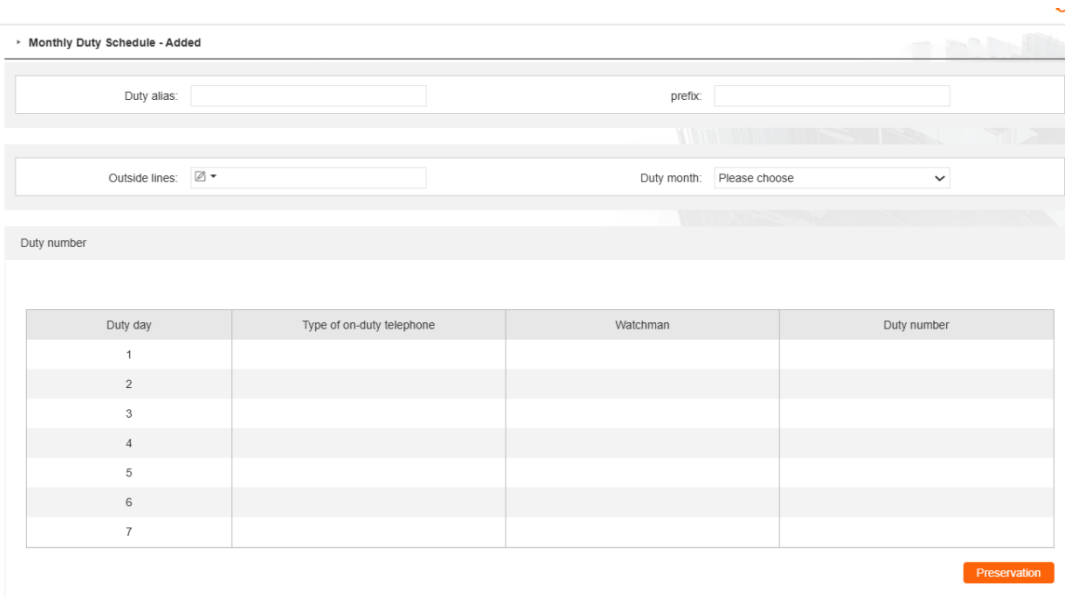


Table3.28 Duty roster Parameter Description

Item	instructions
Duty Alias	Set a name for the duty roster to make it easier to differentiate, e.g. "Beijing Branch Duty by Week".

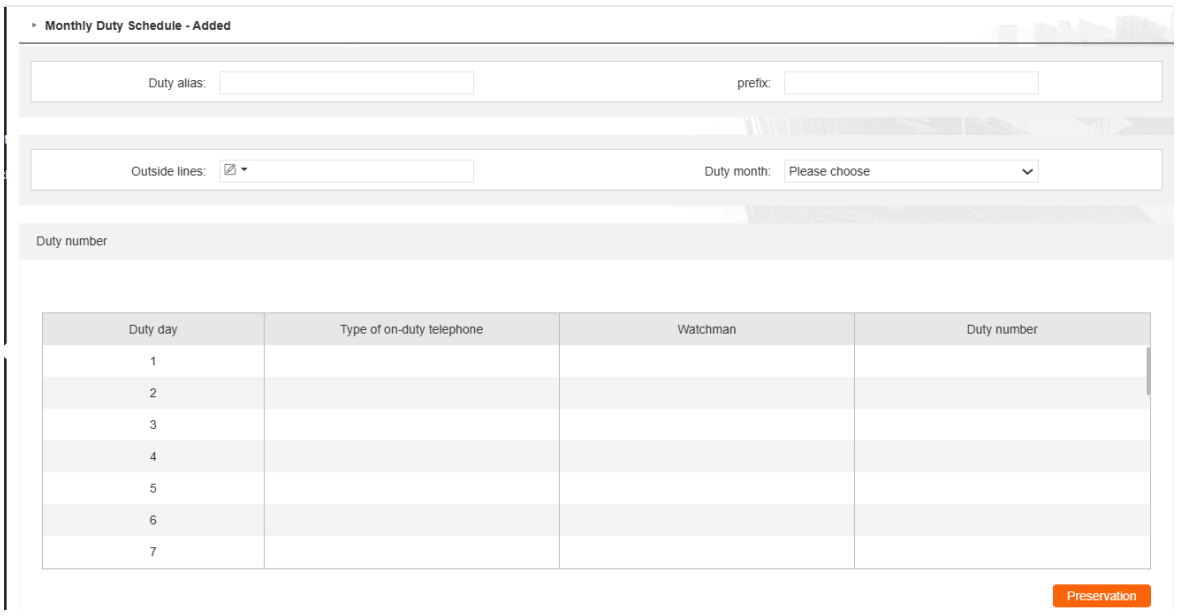
 Copyright © Redstone Systems, Inc

Item	instructions
External Line (E.G. Railway)	Specify the outside line to which this duty roster applies. When there is an incoming call on this outside line, it is transferred to the corresponding duty holder to answer according to the duty list setting.
Prefix (Linguistics)	In the same duty outside the set different duty group dialing code, for example, outside the line when the caller plays the welcome message is "now is the end of the day, consulting product solutions, please dial 1, feedback product problems, please dial 2", then you need to set up two duty table for the outside line, a duty table prefix set to 1, a duty table prefix set to 2. The prefix of one watch is set to 1, and the prefix of one watch is set to 2.
Duty Period	Same as non-working hours configured on theBasic Settings>Switchboardpage.
Watch Number	Click the duty day (e.g., Sunday), select or enter the name of the duty person under "Duty person" (the duty person's name is thename displayedin the IP extension information), and select "Mobile phone or extension, etc." in the drop-down box of "Duty phone type", then the duty number will be automatically generated based on the preset IP extension information. Select "Cell phone or extension, etc." in the "Duty phone type" drop-down box, and the duty number will be automatically generated based on the pre-set IP extension information.

Monthly duty roster

ClickAddto enter the Monthly Duty List Configuration screen, as shown below.

After completing the settings, clickSave. Monthly duty schedules are in effect for the designated month.



 Copyright © Redstone Systems, Inc

Table3.29 Duty roster Parameter Description

Item	instructions
Duty Alias	Set a name for the duty roster to make it easier to distinguish, e.g., "October Duty for Beijing Branch".
External Line (E.G. Railway)	Specify the outside line to which this duty roster applies. When there is an incoming call on this outside line, it is transferred to the corresponding duty holder to answer according to the duty list setting.
Prefix (Linguistics)	In the same duty outside the set different duty group dialing code, for example, outside the line when the caller plays the welcome message is "now is the end of the day, consulting product solutions, please dial 1, feedback product problems, please dial 2", then you need to set up two duty table for the outside line, a duty table prefix set to 1, a duty table prefix set to 2. The prefix of one watch is set to 1, and the prefix of one watch is set to 2.
Duty Month	Select an actual month, e.g. "7" for July.
Duty Period	Same as non-working hours configured on theBasic Settings>Switchboardpage.
Watch Number	Select a duty day, select or search for the name of the duty person under "Duty Person" (the name of the duty person is thename displayedin the IP extension information), and select "Mobile phone or extension, etc." in the drop-down box of "Duty phone type", then the duty number will be automatically generated according to the pre-set IP extension information. If you select "Cell phone or extension" in the "Duty phone type" drop-down box, the duty number will be automatically generated based on the pre-set IP extension information.

Examples:

A company's duty requirements are as follows: Monday and Tuesday non-working hours (including lunch breaks and off-duty time) by the duty officer Lao Li on duty, Wednesday to Friday by the duty officer Lao Wang on duty, New Year's Day holiday by the duty officer Lao Liu on duty. One of them, Lao Li, was on duty with extension 202, while the others were on duty at home with their corresponding cell phones.

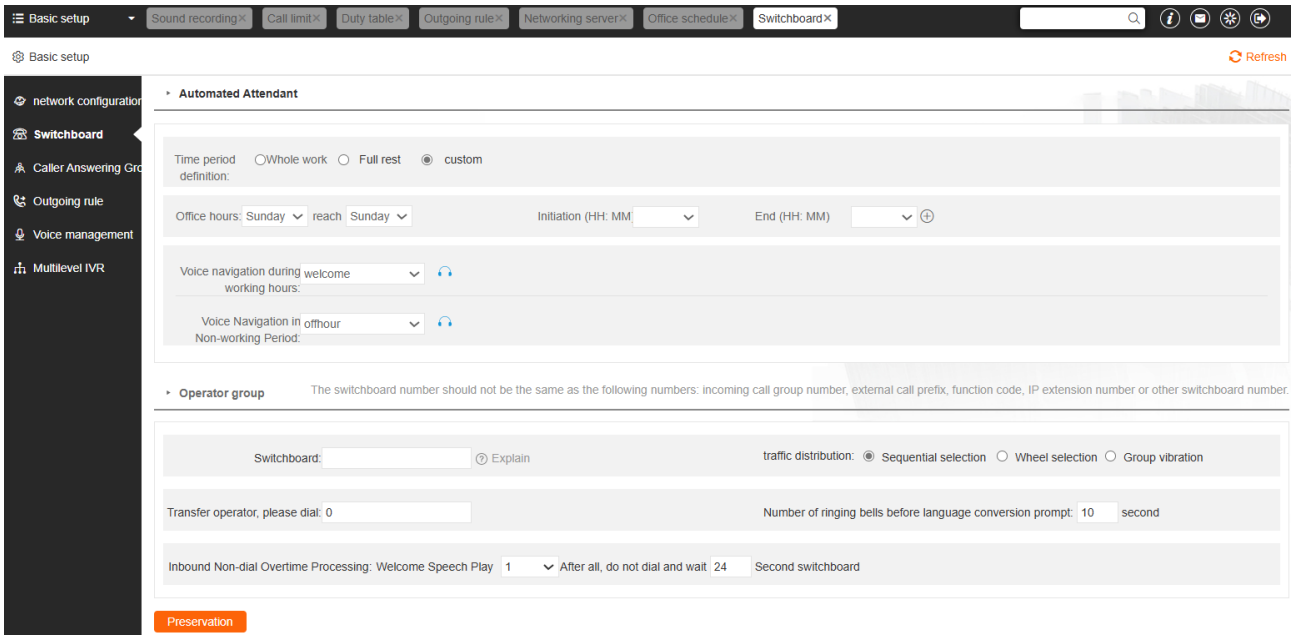
 Copyright © Redstone Systems, Inc

Table3.30 Duty roster Examples

Dates	Out Of Hours, On Duty	External Number (E.G. Telephone)	Duty Officer (Cell Phone/Extension)
Monday To Tuesday	Lunch break: 12:00 - 13:00 Off duty: 18:00 - 09:00 the next day	8888	Old Lee Extension 202
Wednesday To Friday	Lunch break: 12:00 - 13:00 Off duty: 18:00 - 09:00 the next day	8888	Lao Wang cell phone 13900000001
New Year's Day	January 1st.	8888	Lao Liu cell phone 13900000003

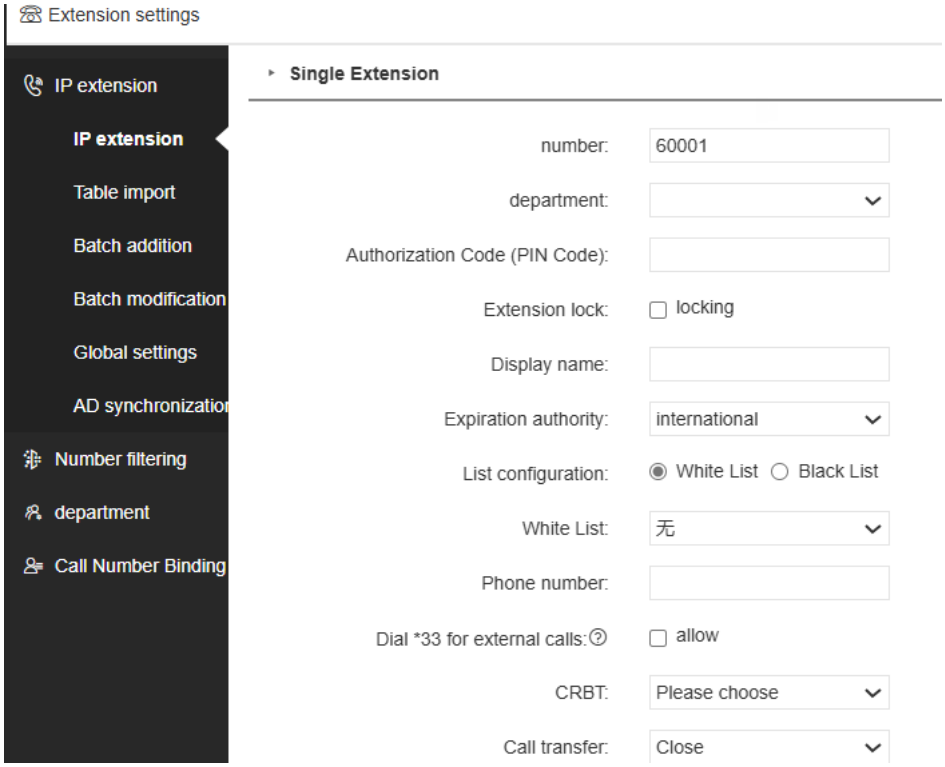
Configuration details:

Step1. Set the working time period at Switchboard>Automated Attendant.



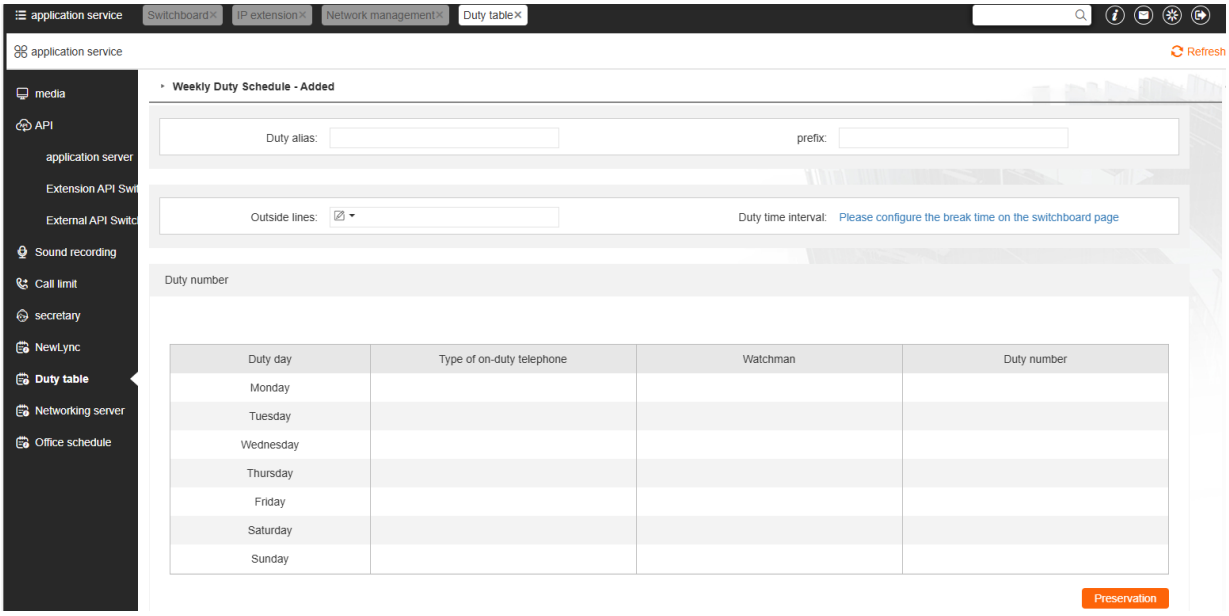
Step2. Confirm that the extension information (including name, extension number, and cell phone number) of the on-duty personnel are all fully configured inExtension Settings>IP Extension.

 Copyright © Redstone Systems, Inc



Step3. Create a weekly duty roster atApplication Services>Duty Roster.

Directly select the Duty Person and Duty Phone Type for Monday through Friday, respectively, and the Duty Number will auto-populate after selection.

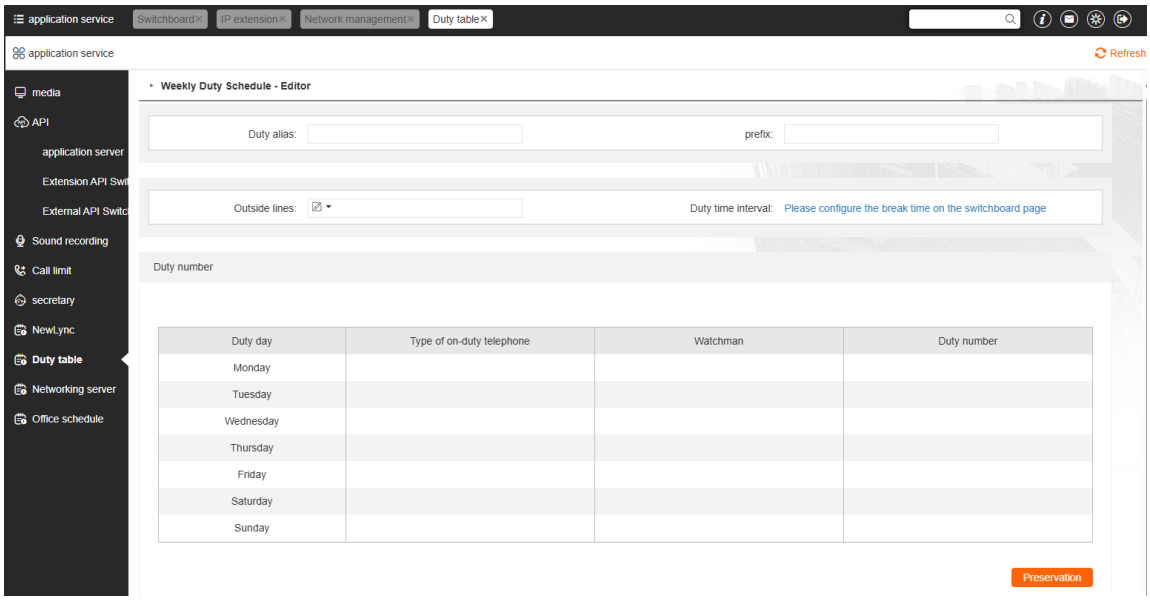


Click Save when you are done configuring.

Step4. Creation of a monthly duty roster

Select #1 and configure the Duty Person and Duty Phone Type, and the Duty Number will

auto-populate.



3.6 Advanced Settings

3.6.1 Systems

Site attribution area code

Step1. Go to Advanced Settings > Systemto set the zone number of the device location.

Figure3-18 Attribution area code configuration screen

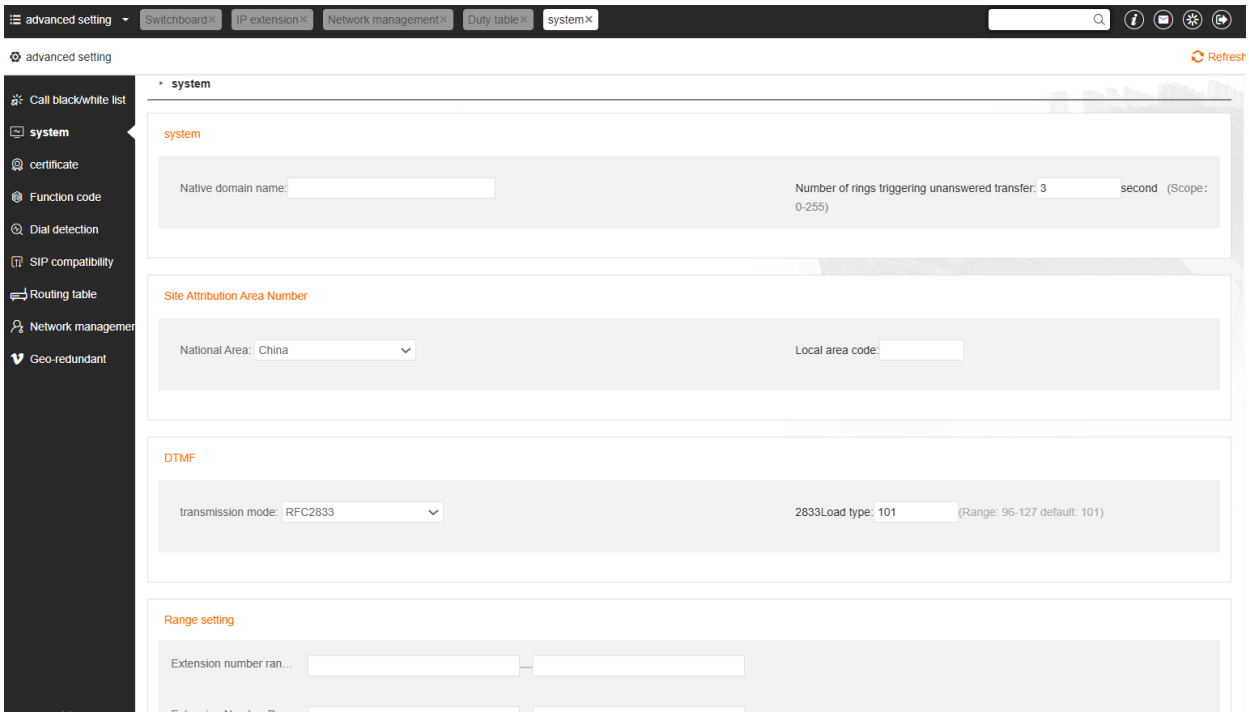


Table3.31 Explanation of attributed area code parameters

Item	Instructions
Local Area Code	Indicates the zone number where the device is located. It is used when the IP outside line operator and the location of the equipment are not the same, the extension dialing habit is still according to the habit in Shanghai. For example, if the device is in Shanghai, fill in 021. When an extension dials a number that does not begin with 0 or 1, the device automatically adds 021 before the number.

Step2. Click Save.

DTMF

Step1. Go to Advanced Settings>Systemto configure DTMF information.

Figure3-19 DTMF interface

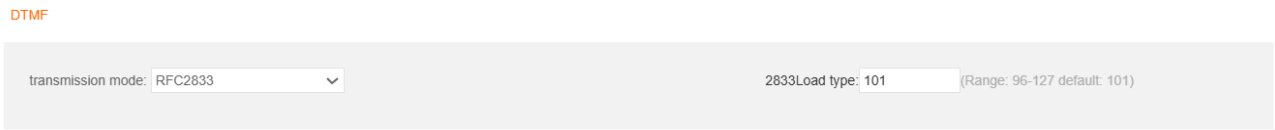


Table3.32 DTMF Parameter Description

Item	instructions
transmission method	The transmission methods of DTMF signals supported by the REX are RFC2833, Transmission, and SIP INFO, and the default is RFC2833. • RFC 2833:Separates the DTMF signal from the voice path and transmits it to the platform via RTP packets in RFC2833 format. • Transmission:The DTMF signal is transmitted to the platform along with the voice path. • SIP INFO:Separates the DTMF signal from the voice path and transmits it to the platform as a SIP signaling INFO message.
2833 Load Type	If RFC 2833 transmission method is selected, you need to configure this item, the value range is 96~127, and the default value is 101. Note that this parameter and the 2833 packet type value supported by the peer (e.g., softswitch platform) should be the same.

Step2. ClickSave.

 Copyright © Redstone Systems, Inc

3.6.2 Certificates

Go to Advanced Settings>Certificates, clickUpload, select the certificate and upload it.



3.6.3 Function Code

Click Advanced Settings>Function Codesto query the system default function codes.

Use the phone to dial a feature code to look up system information or to configure the system.

The function code can be modified by yourself to avoid conflict with extension number, group number of call answering group, transferring switchboard number, prefix number of outgoing call selecting line and other function codes.

Figure3-20 Function Code Configuration Screen

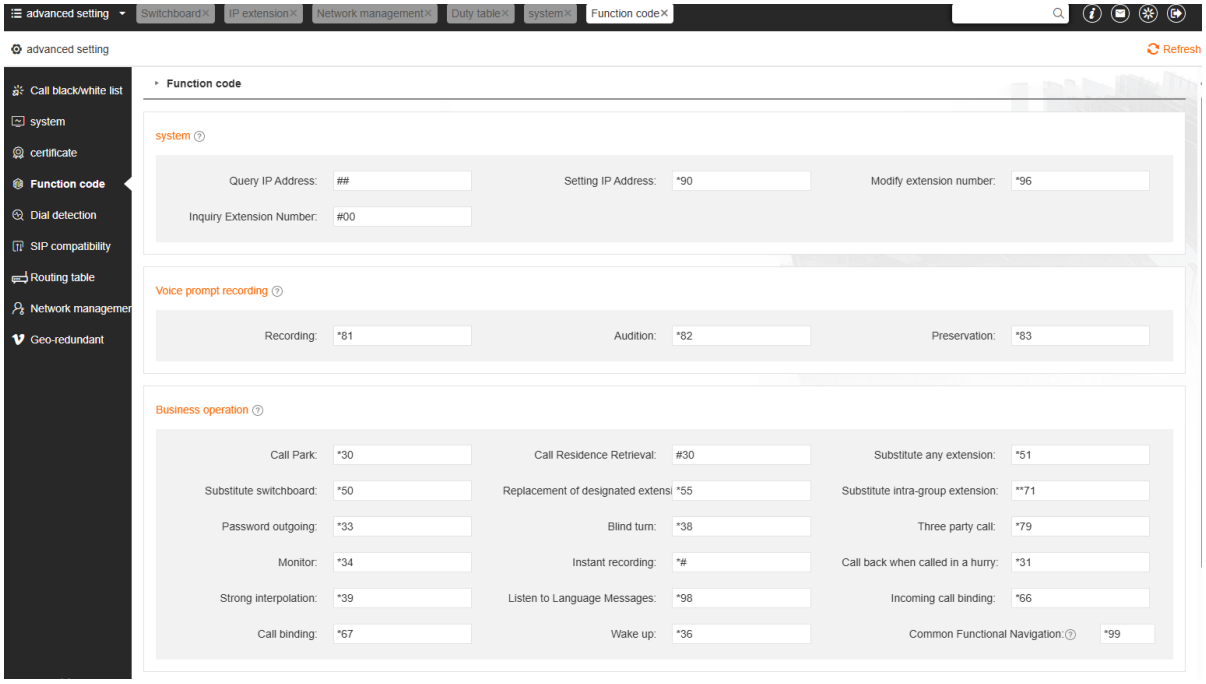


Table3.33 Function code Parameter Description

Item	Instructions
systems	Function code for querying system information.
Voice Prompt Recording	Used for talking heads to record welcome messages. For details on how to use it, see The microphone records a welcome message.
business operation	Function codes are used in the same way for all operation classes: Take off the machine and dial the function code, follow the voice prompts to operate.
Operational Enablement	Function codes are used in the same way for all business enablement classes: Take the machine off the hook and dial the function code, when you hear the voice prompt, it means the function is on.

Note

Feature codes cannot conflict with extension numbers, group numbers of call answering groups, transferring switchboard numbers, outgoing call selector prefix numbers and other feature codes.

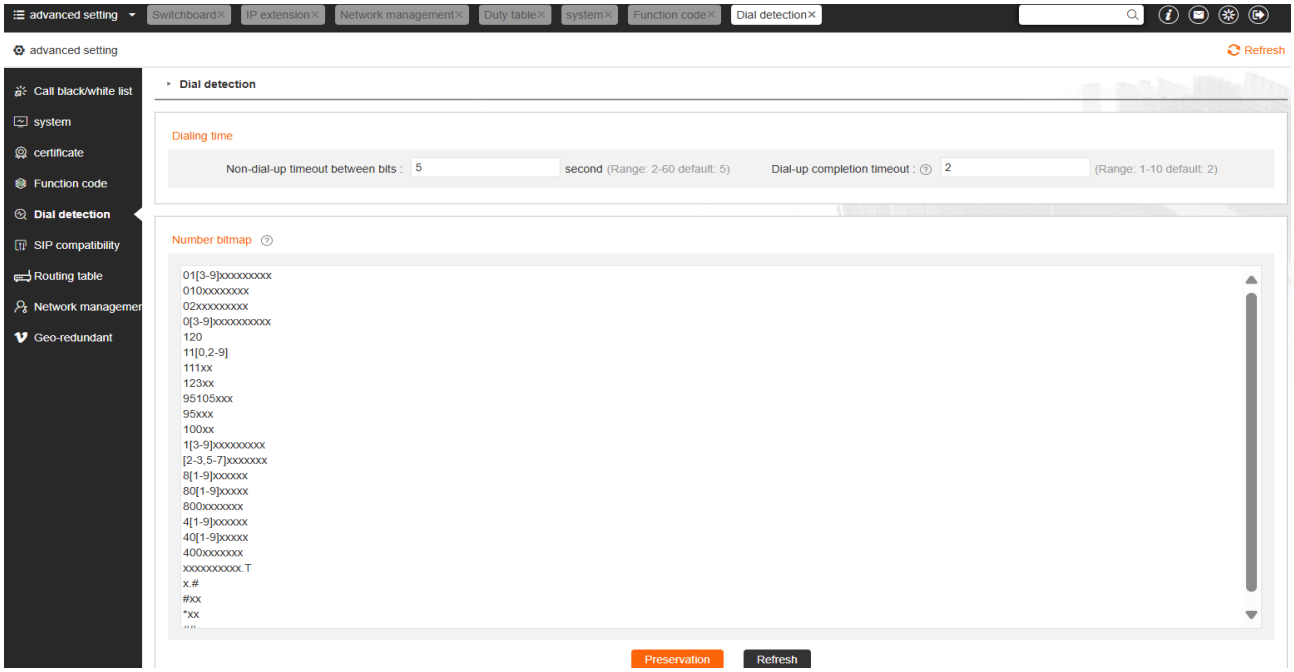
3.6.4 Dial Detection and Bitmap

The device needs to match the detected DTMF number with the number bit chart during the call to determine whether the collection is finished to shorten the delivery time.

ClickAdvanced Settings>Dial Detection,set the rules related to the number bitmap and clickSave.

 Copyright © Redstone Systems, Inc

Figure3-21 Dialing Rule Configuration Screen



The Number Bit Chart can define up to 100 rules, each of which is no more than 50 characters long, for a total string length of no more than 4500 characters. The factory default matching rules cover the rules for the composition of domestic telephone numbers and the function keys used by the device. Users can add new rules as needed. The following are the basic symbols used in the matching rules and instructions for their use.

Table3.34 Explanation of the rules of the common numbered digit map

number plan	Description
Analog extension pickup without dialing timeout	If no number is dialed within the time from off-hook to the time specified in this parameter, the device will abandon this call and play a busy tone to prompt the user to hang up. The default is 15 seconds.
Inter-bit non-dialing timeout	If the next number key is not dialed within the time from the dialing of the previous number key to the time set in this parameter, the device will consider the user's dialing to be finished and call out the dialed number. The default is 5 seconds.
Dialing Completion Timeout	Used in conjunction with the "XXXXXXXXXXXXX.T" rule in the numbered bitmap. The default is 2 seconds.
0-9, *, #	Match specific DTMF signals (corresponding to the dialing keys on the phone).

 Copyright © Redstone Systems, Inc

number plan	Description
x	Match any one bit DTMF signal. E.g. "x" can match "1", "2", etc.
.	Match any number of DTMF numbers. For example, "1." can match any multi-digit DTMF number starting with "1".
T	Timeout terminator. For example, "x.T" means that after receiving one or more numbers, no DTMF signal is received within the specified time, and the matching is finished.
[ ]	Matches the DTMF signal set. For example, "[1-3, 5, 7-9]" can match any of "1, 2, 3, 5, 7, 8, 9".
xxxxxxxxxxx.	For numbers up to and including 10 digits, if no new number is received within the inter-digit non-dialing timeout period, the device ends the collection; for numbers above 10 digits, if no new number is received within the dialing completion timeout period, the device ends the collection.
x.#	Receiving any digit number and then receiving "#" immediately ends the receipt of the number.
[2-8] xxxxxxxx	Receiving an 8-digit number starting with any number between 2 and 8 ends the collection. Used to define local calls.
02xxxxxxxx	Receiving an 11-digit number starting with 02 ends the collection. Used to define long distance calls beginning with 02.
013xxxxxxxx	Receiving a 12-digit number starting with 013 ends the collection. Used to define long distance cell phone calls that begin with 013.
13xxxxxxxx	Receiving an 11-digit number beginning with 13 ends the collection. Used to define cell phone calls that begin with 13.
11x	Receiving a 3-digit number starting with 11 ends the collection.
9xxxx	Receiving a 5-digit number starting with 9 ends the collection.

 Copyright © Redstone Systems, Inc

3.6.5 SIP Compatibility

Step1. Go toAdvanced Settings> SIP Compatibilityto set the SIP compatibility information.

Figure3-22 SIP Compatibility Interface

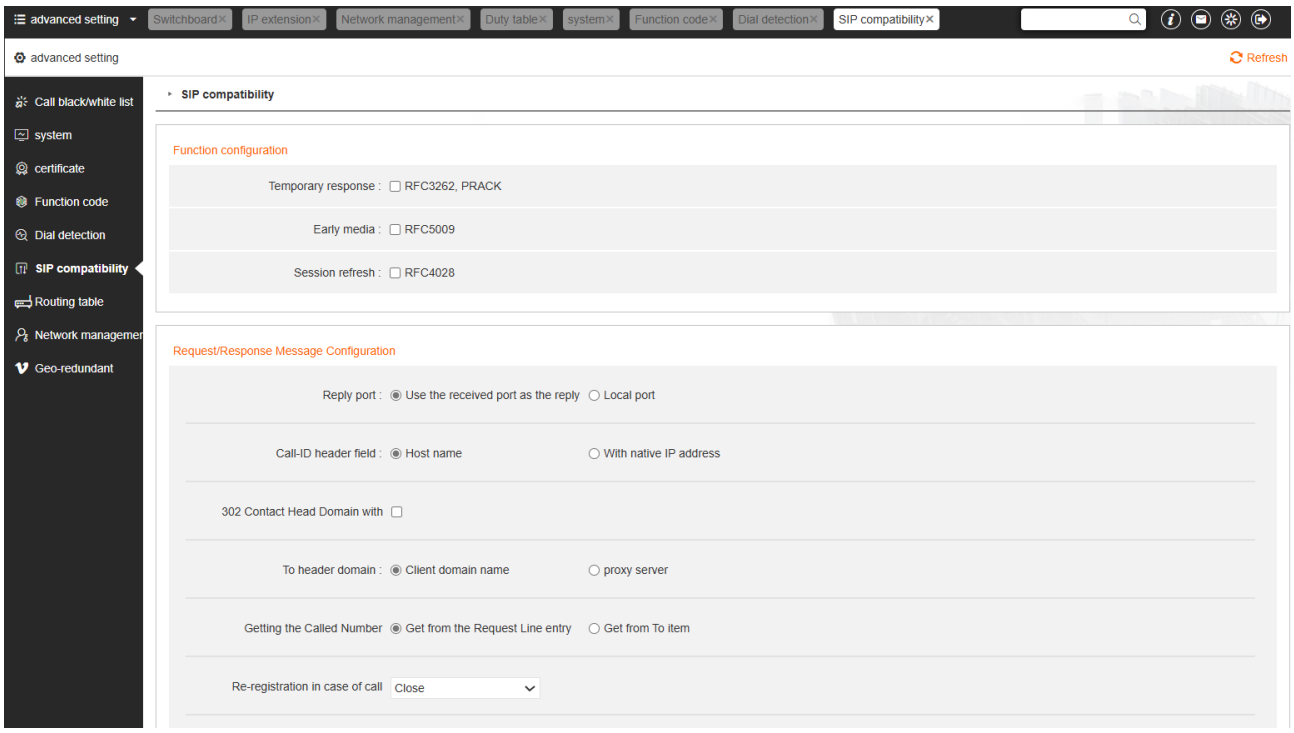


Table3.35 SIP Compatibility Parameter Description

Item	Instructions
Interim Response	Open RFC3262, PRACK. The system default is unchecked.
Early Media	Open RFC5009. The system default is unchecked.
Media Stream Direction Attributes	Note: This can be configured whenEarly Mediais checked. Configure the parameter values for the P-Early-Media header field for early media as follows: • Supported • Sendrecv • Sendonly • recvonly • Inactive The fields carried in different mode SIP messages are different. Selection is based on the requirements of the opposite end.

 Copyright © Redstone Systems, Inc

Item	Instructions
Session Refresh	Session Refresh (RFC4028) uses periodic re-INVITE or UPDATE requests and corresponding response messages during a call to determine if the call is "alive" so that resources can be released in a timely manner. When the sender of a session refresh request (the refresher) does not receive a response or the receiver of the request does not receive a refresh request within the refresh cycle, it assumes that the other party does not exist, ends the call, and releases the resources. The refresher and refresh period are determined by negotiation between the parties involved in the call, including both parties to the call and the various agents en route. The refresh period (which is carried in the Session-Expires header field) must not be less than the Minimum Refresh Request Interval (which is carried in the Min-SE header field). The device disables session refresh by default. When there is an imperfect resource release mechanism in the call-related parties (e.g., no RTP stream detection mechanism, no BYE request timeout detection mechanism, etc.), it is recommended to enable the session refresh function. With the session refresh feature turned on: When the device acts as the calling party, it carries the session refresh related header field in the INVITE message it sends, and when the device acts as the called party, it responds to a request that carries the session refresh header field by inserting the final session refresh period and the proposed refresher in the 200 OK message to complete the negotiation.
Refresh Request Interval	That is, the session refresh cycle, the device will carry the value in the Session-Expires header field in the INVITE or UPDATE message. The default is 1800 seconds, with a range of values from 30 to 65535 seconds.
Minimum Refresh Request Interval	The minimum session refresh period that the device can accept. The default is 1800 seconds, with a range of values from 30 to 65535 seconds. The final negotiated session refresh period cannot be less than this value.
Response Ports	Select the reply port for SIP messages. The system defaults to "use the received port as the reply port".
To Header Fields	Select whether to use the client domain name or proxy server for the To header value, the system defaults to "Client Domain Name".
Call-ID Header Field	Select whether the Call-ID header field should have a host name or a local IP address, the system default is "with host name".
How To Get The Called Number	Select to get the called number from Request Line header field or To header field, the system default is "Get from Request Line item".

 Copyright © Redstone Systems, Inc

Item	Instructions
302 Contact Header Field With Destination Number	Used to control whether the destination number of the call transfer carried in the Contact header field of the 302 message sent by the device when the call is transferred contains the prefix added in the routing rule. This parameter is valid only when the following conditions are both present: • Parameter FT_FAT_X=on is set for IP outside line • This IP outside line sets the DID to the extension • The corresponding DID extension is set up for call forwarding to an external number, e.g. to the target number 13812345678 • A routing rule exists that defines the prefix to be added when calling out to this destination number over an IP outside line, such as the routing rule FXS 138 ADD 9 Check this parameter, the destination number carried on the Contact header field in the 302 message sent by the device contains the prefix 9 in the routing rule, which is 913812345678, and if it is unchecked, it does not contain the prefix, which is 13812345678.

Step2. Click Save.

3.6.6 Routing Table

The routing table is used to implement number substitution and route assignment with a capacity of 500 entries and is executed in top-down order.

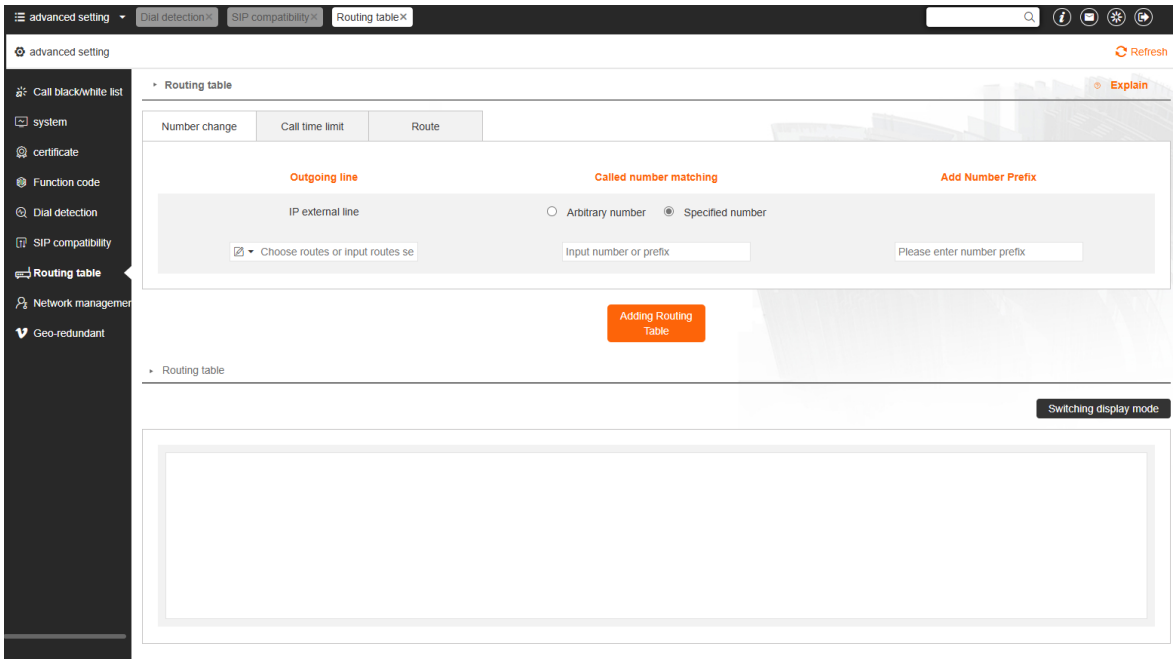
Go toAdvanced Settings>Routing Tableto add routing rules.

Specific instructions are given below.

 Copyright © Redstone Systems, Inc

Number Conversion

Figure3-23 Routing Table Configuration Interface



There are two ways to configure routing rules. One is to enter the command in the space below the routing table, and the other is to configure it in the configuration area above. To make it easier to explain the meaning of routing, the way to enter commands is described first.

1. Command writing rules: outside line type*called prefix*ADD*add prefix*

This rule is used to automatically add a prefix to a called number that matches to the*called prefix*on an outgoing call.

Description: Outbound type FXS means outbound via IP outbound.

- IP outbound call, called add prefix 17909

  FXS *X* ADD *17909*

- IP outbound calls to called numbers beginning with 10, add prefix 17909

 Copyright © Redstone Systems, Inc

FXS *10* ADD *17909*

2. Interface Configuration Rules

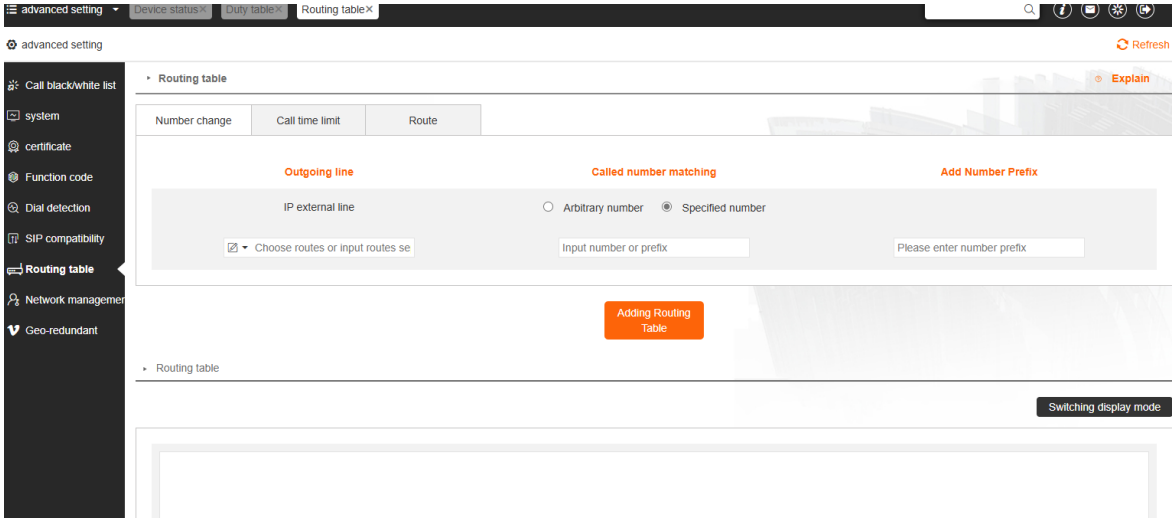


Table3.36 Interface Configuration Rules Description

Item	instructions
out of bounds (sports)	Tap the drop-down arrow in the input box below to choose to enter the number yourself, or select the number from the list of numbers.
Called Number Matching	It can be any number, or specify the prefix of the called number.
Add number prefix	The prefix entered here will be added before the final called number.

Example:Add the prefix 9 to the called for all outgoing callsfromIP outside line 62203005.

Configuration method:

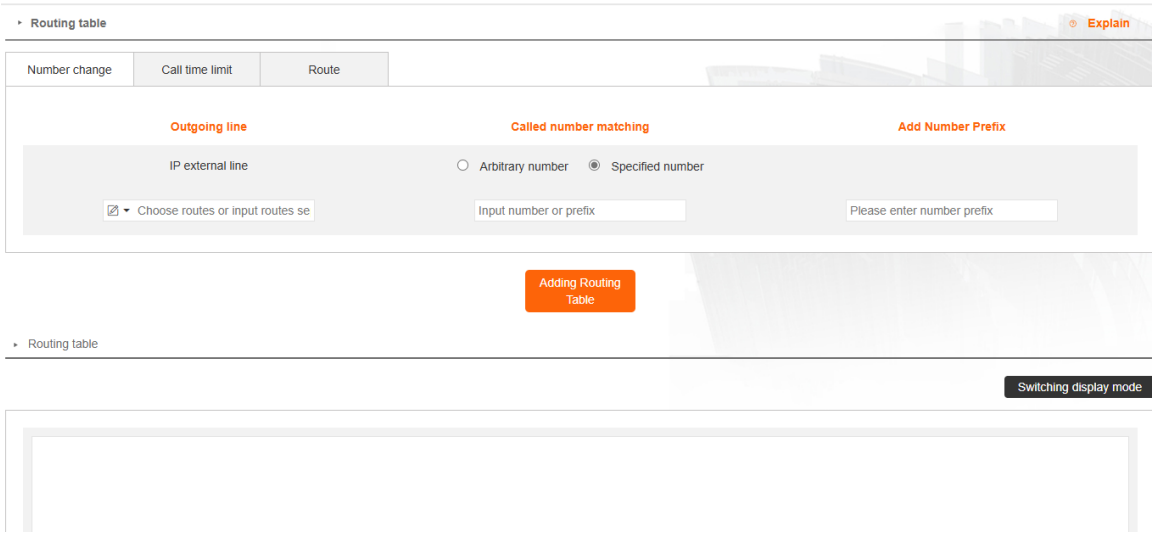
For outgoing line 62203005, select any number for the called number and enter "9" in the number prefix field.

1.ClickAdd to Routing Table.

2.The final generated routing rule: FXS[62203005] X ADD 9, which will appear in the routing table below.

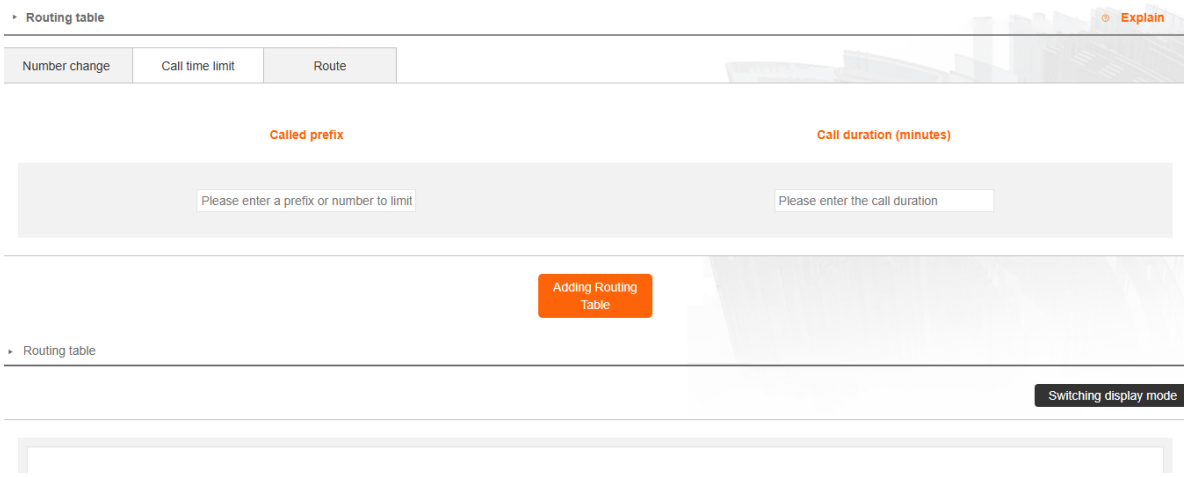
3.Finally, clickSave.

 Copyright © Redstone Systems, Inc



Outgoing Time Limit

Figure3-24 Routing Table Configuration Interface - Call Length Restriction



There are two ways to configure routing rules. One is to enter the command in the space below the routing table, and the other is to configure it in the configuration area above. To make it easier to explain the meaning of routing, the way to enter commands is described first.

1. Command writing rules:

   FXS *Called Prefix*TIME*Individual call duration limit/total duration/type/remaining duration*

Where the remaining hours are calculated by the system and do not need to be configured.

 Copyright © Redstone Systems, Inc

Note: The call duration restriction rule starts with "FXS" regardless of whether the originating extension is an analog or IP extension.

This rule is used to limit the duration of outgoing calls that match to the called prefix.

Type: D or M, D for daily and M for monthly

Examples:

- Calls to a specified caller (e.g., international calls, i.e., called numbers beginning with 00), with a limit of 100 minutes per day, unlimited for individual calls

  Configuration: FXS *00* TIME *0/100/D*

  Display: FXS *00* TIME *0/100/D/100*

2. Interface Configuration Rules

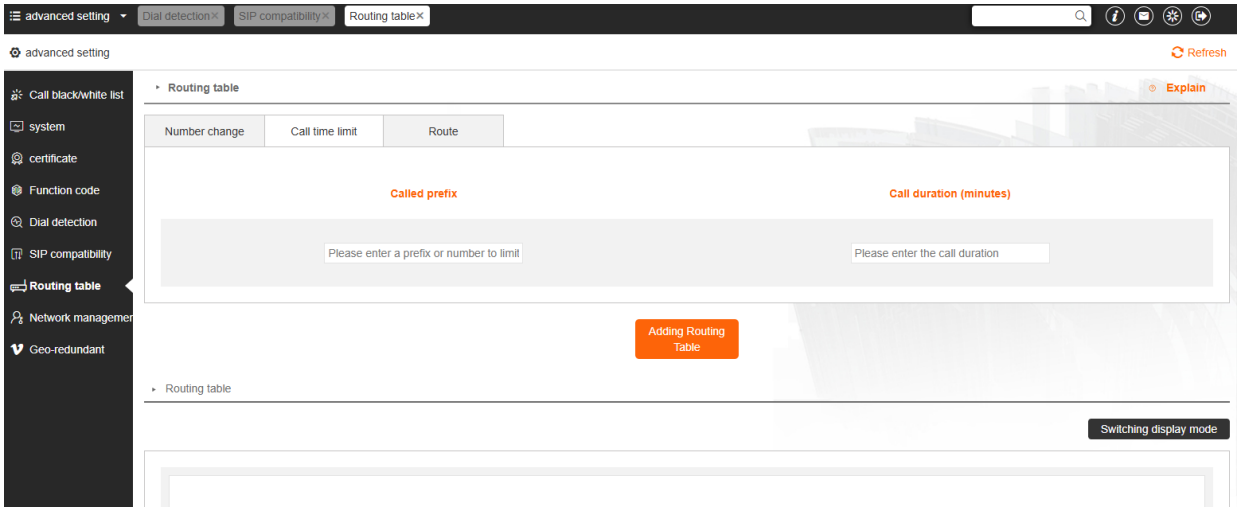


Table3.37 Interface Configuration Rules

Item	instructions
called prefix	The called number of the call matches this prefix, then the call limits the call duration according to the rules.
call duration	Enter the total duration, for example, if the total call duration for the called number whose call is matched to the prefix is 100 minutes, enter 100.

Example:The total call duration for international calls is limited to 100 minutes.

 Copyright © Redstone Systems, Inc

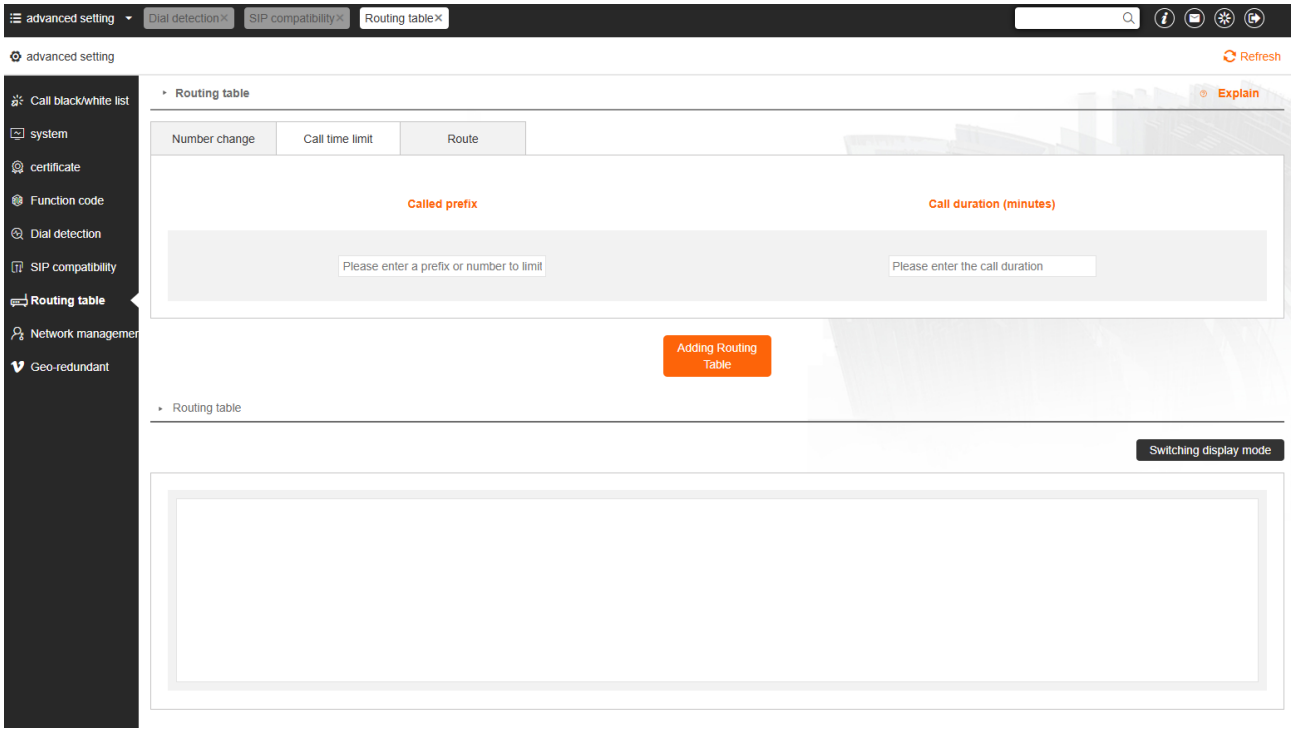
Configuration method:

Enter "00" for the called prefix and "100" for the call duration.

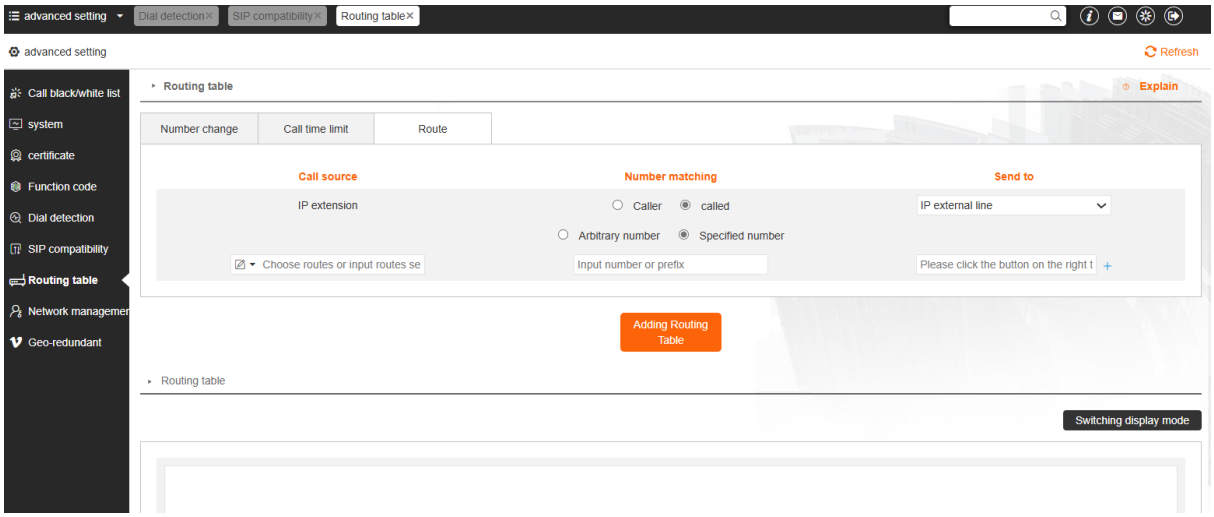
1.ClickAdd to Routing Table.

2.The final generated route, FXS 00 TIME 0/100/D, appears in the routing table below.

3.Finally, clickSave.



Directional Routing



There are two ways to configure routing rules. One is to enter the command in the space below the routing table, and the other is to configure it in the configuration area above. To make it easier to explain the meaning of routing, the way to enter commands is described first.

1. Command Writing Rule:FXS *Called Prefix*ROUTE*Route Destination*

Used to specify a routing destination for outgoing calls that match to*the called prefix*. This function requires the outgoing call rule to set the route selection method to "Route" mode.

Note: Directional routing rules are fixed to start with "FXS". IPT (for IP outside line), IP (for specific IP address).

Examples:

- Calls to the designated callee (e.g., beginning with 6120) are delivered to IP outside lines 1 through 6 in the down-selected manner

  FXS *6120* ROUTE *IPT 1~6*

- Calls to a specified callee (e.g., beginning with 6120), delivered to IP address

192.168.2.218

FXS *6120* ROUTE *IP 192.168.2.218*

2. Interface Configuration Rules

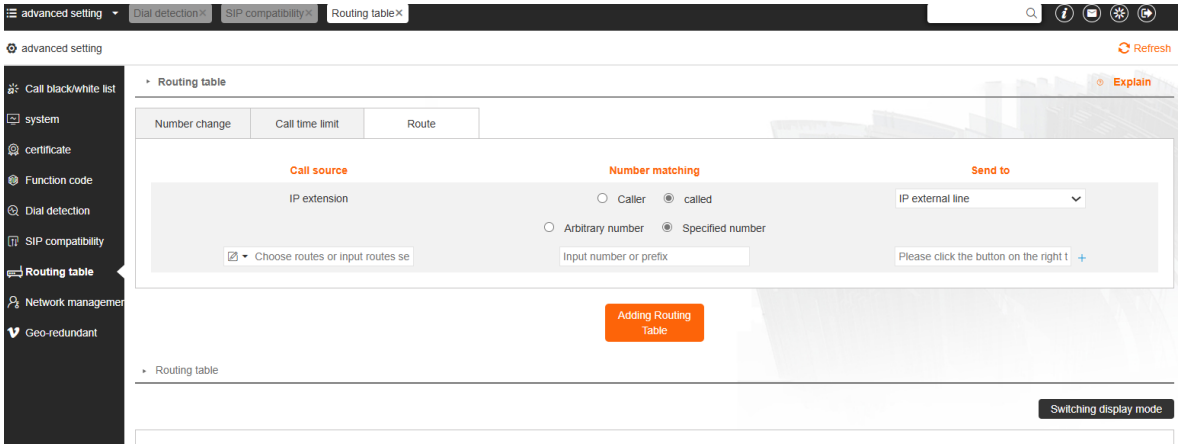


Table3.38 Interface Configuration Rules

Item	Description
Call Source	A call originating from a specified extension is indicated by first selecting an analog extension or an IP extension, and then specifying the specific extension with the plus sign to the right of the input box below.
Number Matching	Match the calling or called number. Enter a prefix in the input box below thespecified number, then the prefix will be used to match the calling or called number, and the routing rule will be executed for the matched number.
Send To	Select the outgoing line, IP outside line, IP address or POS/Modem pass-through, and also click + to select a specific line.

Example:A call to a specified called (e.g., beginning with 6120) selects an IP outbound outgoing line according to the down-select method.

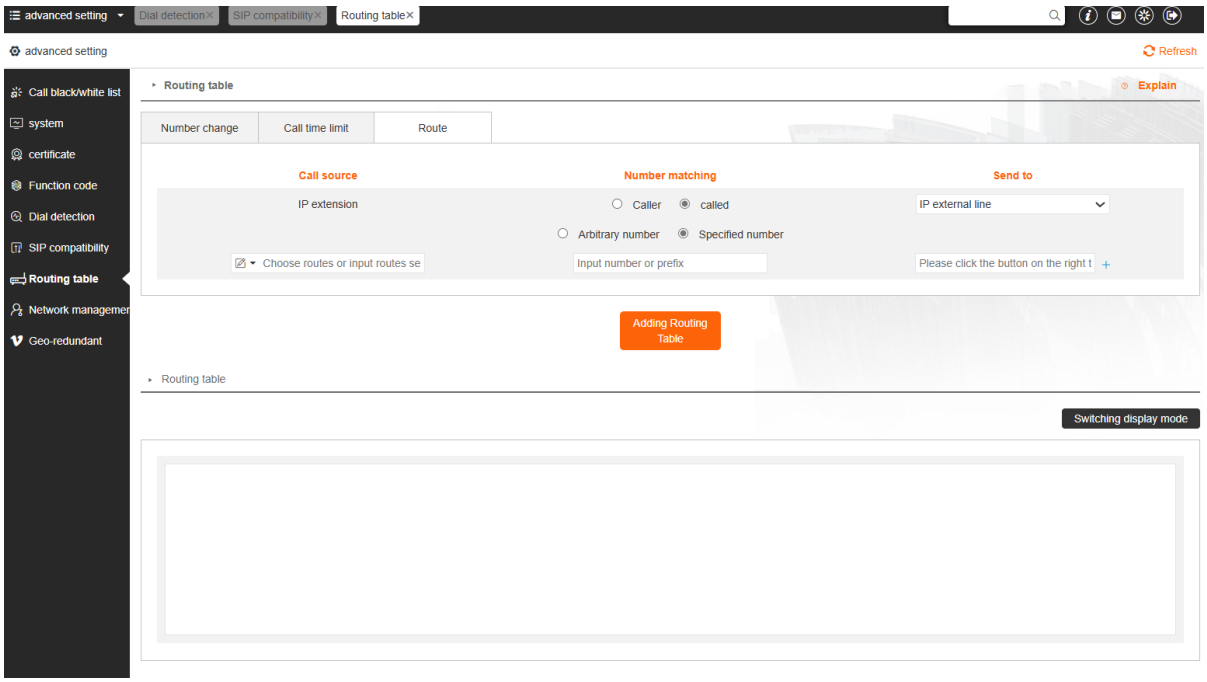
Configuration method:

No need to select thecall source, select "Called" "Assigned Number"for number matching, and enter "6120" in the input box below.

The final generated route:the FXS 6120 ROUTE IPT, appears in the routing table below.

 Copyright © Redstone Systems, Inc

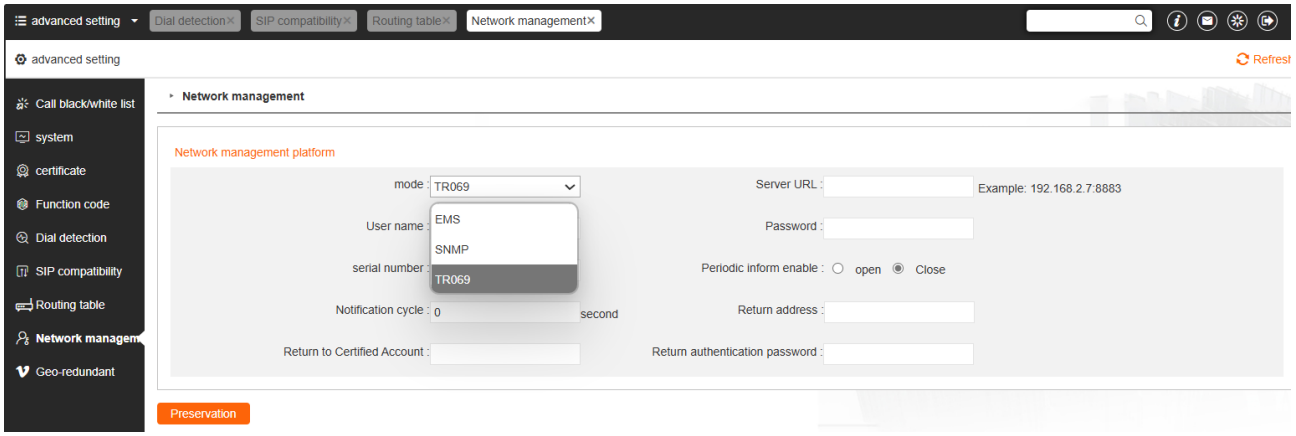
Finally, click Save.



3.6.7 Network Management

EMS

Step1. Go toAdvanced Settings>Webmasterand configure the server URL after selecting EMS.



Step2. ClickSave.

TR069

Step1. Go toAdvanced Settings>Network Managementand select TR069 to configure.

Figure3-25 TR069 Configuration Interface

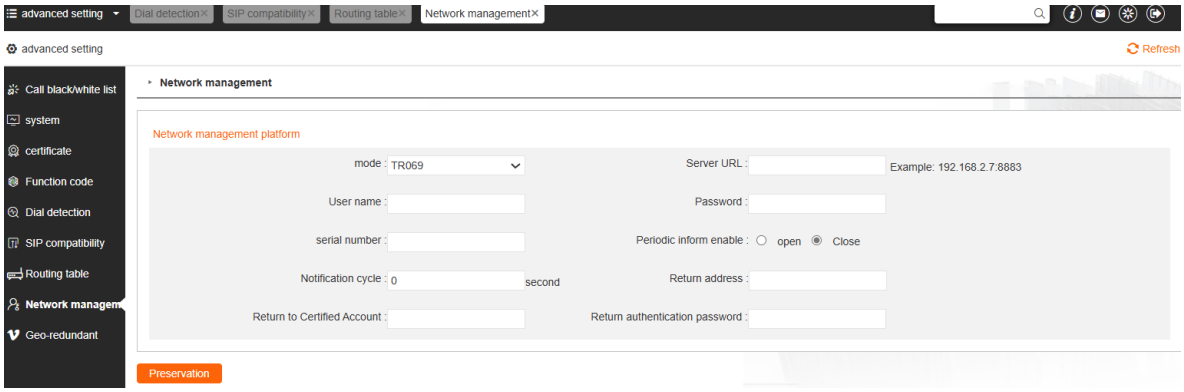


Table3.39 TR069 Parameter Description

Item	Description
Server URL	Set the URL of the webmaster server.
user ID	Set the user name used for authentication with the network management server.
cryptographic	Set the password used for authentication with the network management server.
product key (software)	The serial number of the product, which defaults to the MAC address of the Swift. When interfacing with the operator's network management server, you can fill in the serial number provided by the other party. Generally, this may not be completed.
Periodic notification switch	A switch that reports periodically to the network management server.
notification period	The interval for reporting to the network management server.
return address	The address of the network management server's back-connected device. Generally generated automatically, you can also manually fill in the address of the device.
Backlink Certified Account	The account number of the network management server's back-connected device.
Reconnect Authentication Password	The password for the network management server to connect back to the device.

Step2. Click Save.

 Copyright © Redstone Systems, Inc

SNMP

Step1. Go toAdvanced Settings>Network Managementto configure it.

Figure3-26 SNMP Configuration Interface

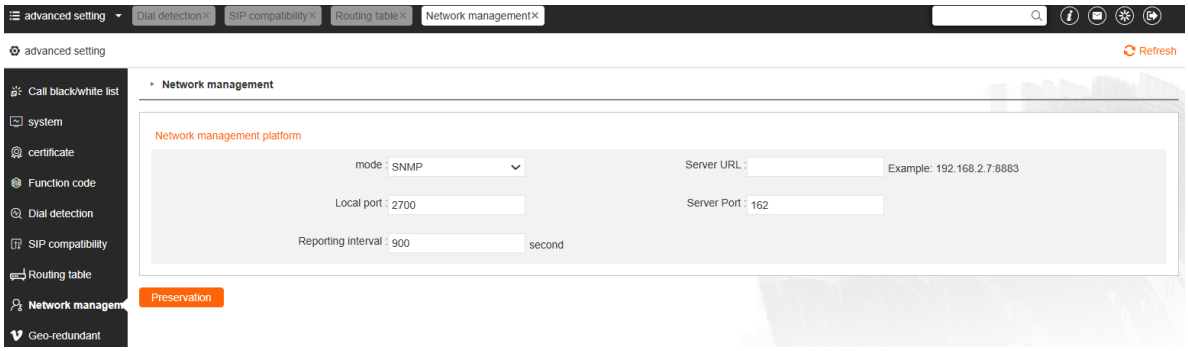


Table3.40 SNMP Parameter Description

Item	Description
Server URL	Set the URL of the webmaster server.
local port	Enter the SNMP local port. The default is 2700. If you select the SNMP method, you need to fill in the following three parameters.
server (computer)	Enter the SNMP server address.
server port	Enter the SNMP server port number. The default is 162.
Reporting intervals	Unit is in seconds. The default is 900 seconds.

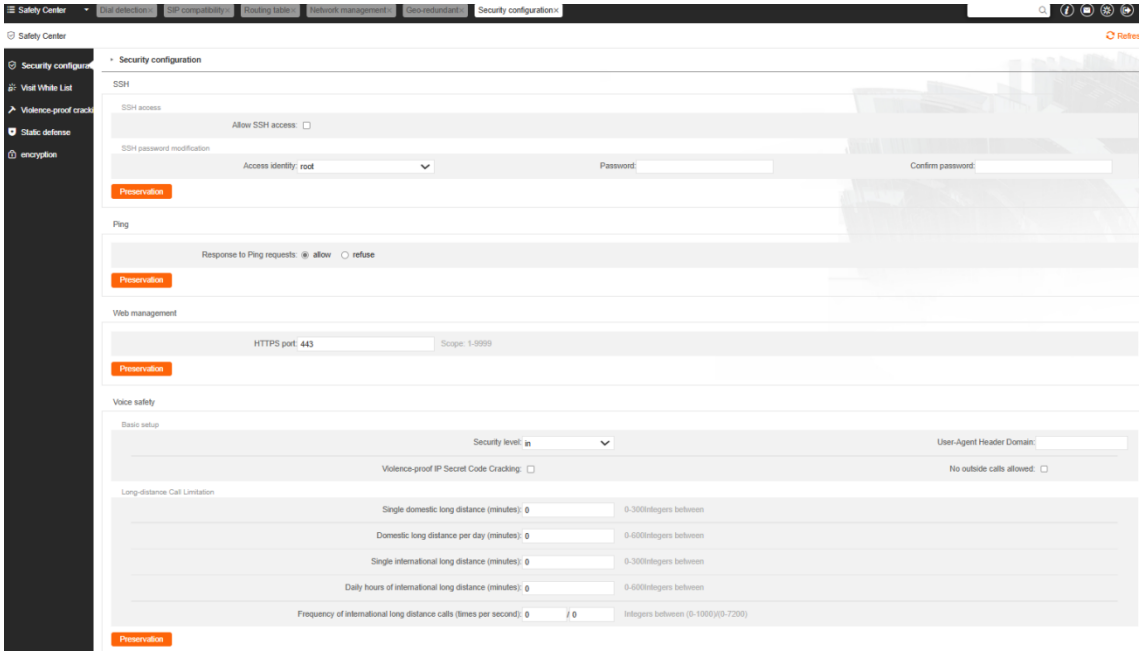
Step2. Click Save.

 Copyright © Redstone Systems, Inc

3.7 Security Center

3.7.1 Safety Configuration

Go toSecurity Center>Security Configuration.



SSH

Go to Security Center>Security Configurationand turn on SSH.

The device shipped with SSH turned off by default. If there is no special need, it is recommended to close it.

Table3.41 SSH Configuration Interface

Item	Description
Ssh	Check the box to allow access to the device via SSH. Default off. SSH access is only possible by logging in as operator and then switching to the root user via the su root command. SSH needs to be closed promptly after use.
SSH Port	The default is 22, which can be modified.
Access Identity	Both operator and root access rights.

Item	Description
Password / Confirm Password	Change the root user/operator user password for SSH access. Passwords are subject to the following requirements: ● Length 6~20 characters ● Use a combination of letters plus numbers or special symbols for passwords ● No &, = or " " signs can be entered.

Ping (name)

Go toSecurity Center>Security Configurationand configure to allow or disallow being pinged.

By selecting Deny, the device will not respond to Ping messages, thus circumventing malicious attacks.

Table3.42 Responding to Ping Requests Parameter Description

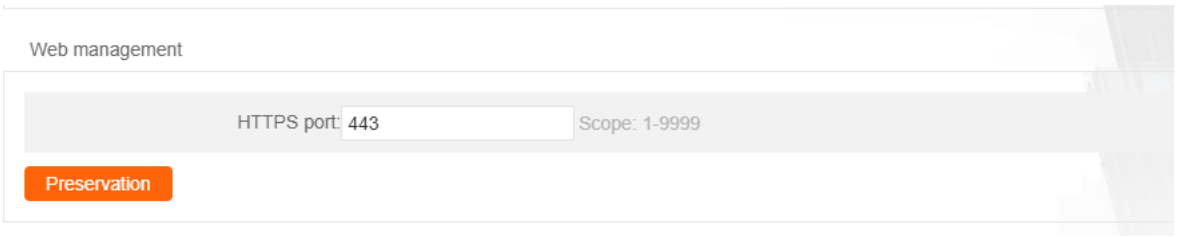
Item	Description
Responding to Ping Requests	Allow: the device receives a Ping request and responds. Forbidden: the device does not respond to any ping requests.

Web Management

The device supports access to the web interface via the HTTPS protocol.

Go to Security Center>Security Configurationto configure the Web access port. This function takes effect after reboot.

Figure3-27 Web Management Configuration Interface



 Copyright © Redstone Systems, Inc

Table3.43 Web Management Interface Parameter Description

Item	Description
HTTPS port	Set the Web port when accessing the device using the HTTPS protocol, the default value is 443, value range: 1~9999.

Voice Security

Go to Security Center>Security Configuration to configure voice security related features.

Figure3-28 Voice Security Configuration Interface

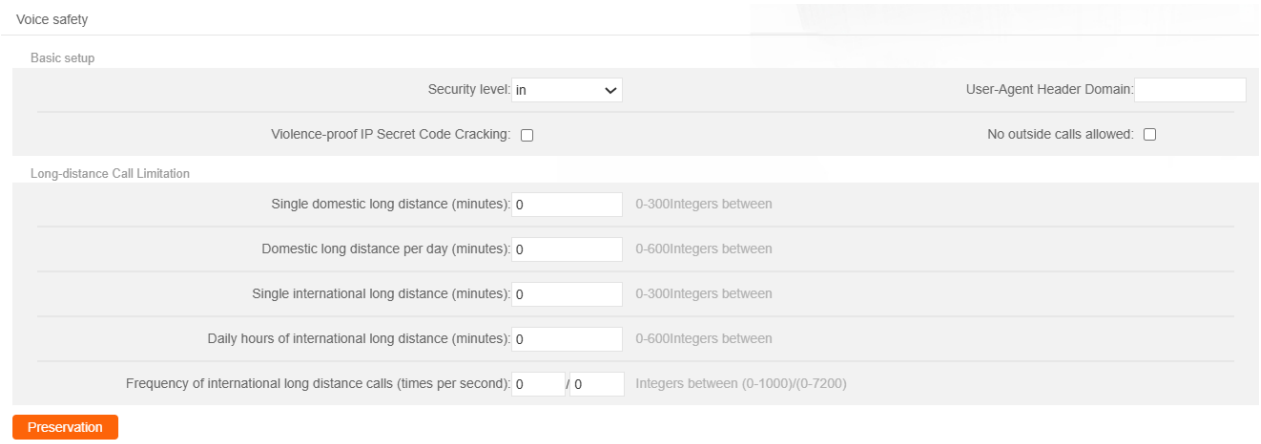


Table3.44 Description of voice security interface parameters

Item	Instructions
(Military) Rank	The restrictions under each security level are listed below: • High:Intranet IP extensions with SIP signaling ports greater than 10000 and the same registration password and number are not allowed to register; extranet IP extensions with the same registration password and number are not allowed to register; extranet terminals are not allowed to log in to the Web management interface. • Medium:Same as the above restriction, but allows external network terminals to log in to the Web management interface. • Low:None of the above limitations.
Prohibit Calls To Outside Lines	Prohibit outside IP extensions from calling outside lines, i.e., outside IP extensions are only allowed to call extensions.
User-Agent Header Fields	Enter the client User-Agent header fields that are allowed to be registered, separated by "," if there is more than one. If this configuration is not empty, IP extension registration needs to carry the same User-Agent header field, otherwise registration will fail.
Prevent Brute Force Breaking Of IP Extension Passwords	When IP extension authentication fails more than the number of times specified in this parameter, the device will reject the registration of the IP extension. This IP extension is allowed to register only if the IP address of this extension is changed or the REX is restarted.
Long Distance Call Restriction	

 Copyright © Redstone Systems, Inc

Item	Instructions
Single Domestic Long Distance Hour	Maximum length of a single domestic long-distance call.
Domestic Long-Distance Hours Per Day	The maximum value of the total duration of all domestic long-distance calls in a day.
Single International Call Duration	Maximum length of a single domestic long-distance call.
Hours Per Day For International Calls	The maximum value of the total duration of all international calls in a day.
Frequency Of International Calls	Maximum number of international calls initiated per second.

3.7.2 Access To A White List

White listing is used to configure the IP addresses that are allowed to access the device's Web or SSH services.

With white listing enabled, only whitelisted IP addresses are allowed to access OM's Web or SSH services.

The configuration steps are as follows:

Step1. Go toSecurity Center>Access Whitelist, clickAdd, and fill in the whitelist information. The device can add up to 20 addresses.

Figure3-29 Whitelist Configuration Screen

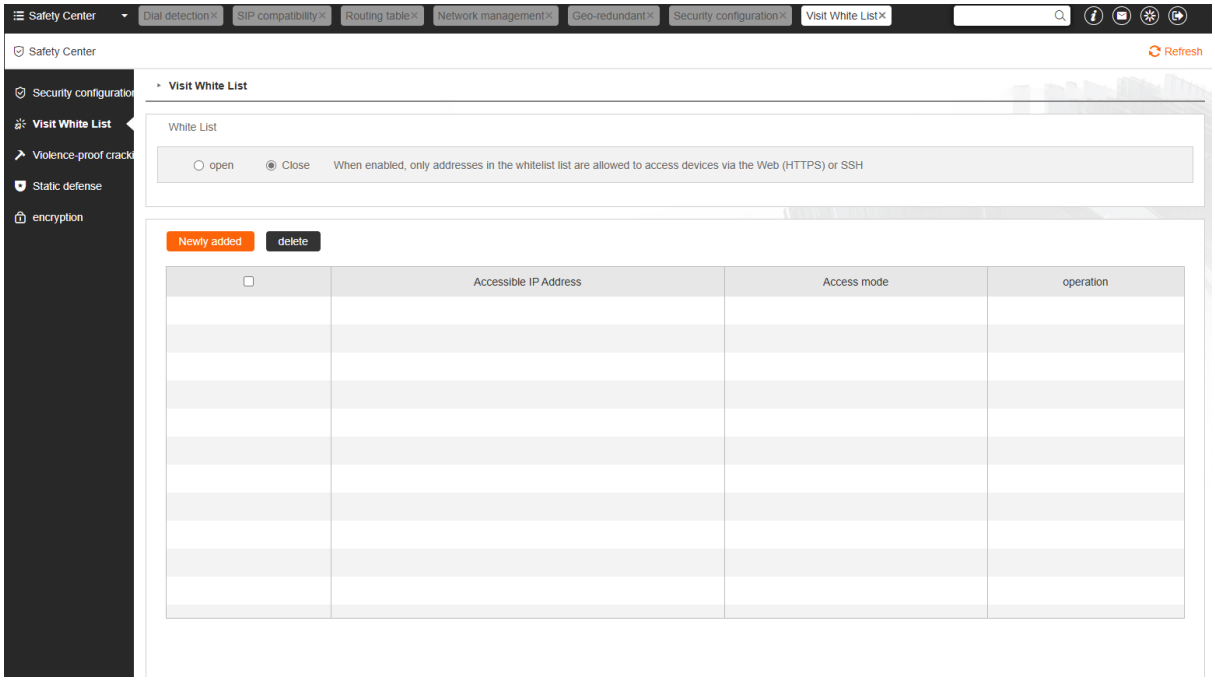


Table3.45 Description of whitelisting parameters

Item	instructions
IP addresses allowed to access	Fill in the IP address that is allowed to access the device.
access method	Select the services that are allowed to be accessed, optionally SSH, HTTPS, etc.
removing	Delete the current whitelist information.

Step2. Save the settings.

Step3. Turn onwhitelisting.

Note

To access the device via SSH, you also need to enable the SSH service for the device on theSecurity>Security Configurationpage.

3.7.3 Brute Force Account Cracking Prevention

The main manifestation of a brute-force account is multiple login attempts by the same attack source in a short period of time. In response to the characteristics of this attack, the device provides a combination of verification code authentication, limiting the number of failed login attempts and access whitelisting for Web logins to eliminate brute-force cracking at the source.

Login Retry Locked Configuration

After logging in, clickSecurity Center>Anti-Violence Breach Accountsto open this configuration screen.

Figure3-30 Brute force account (login retry lockout) configuration screen

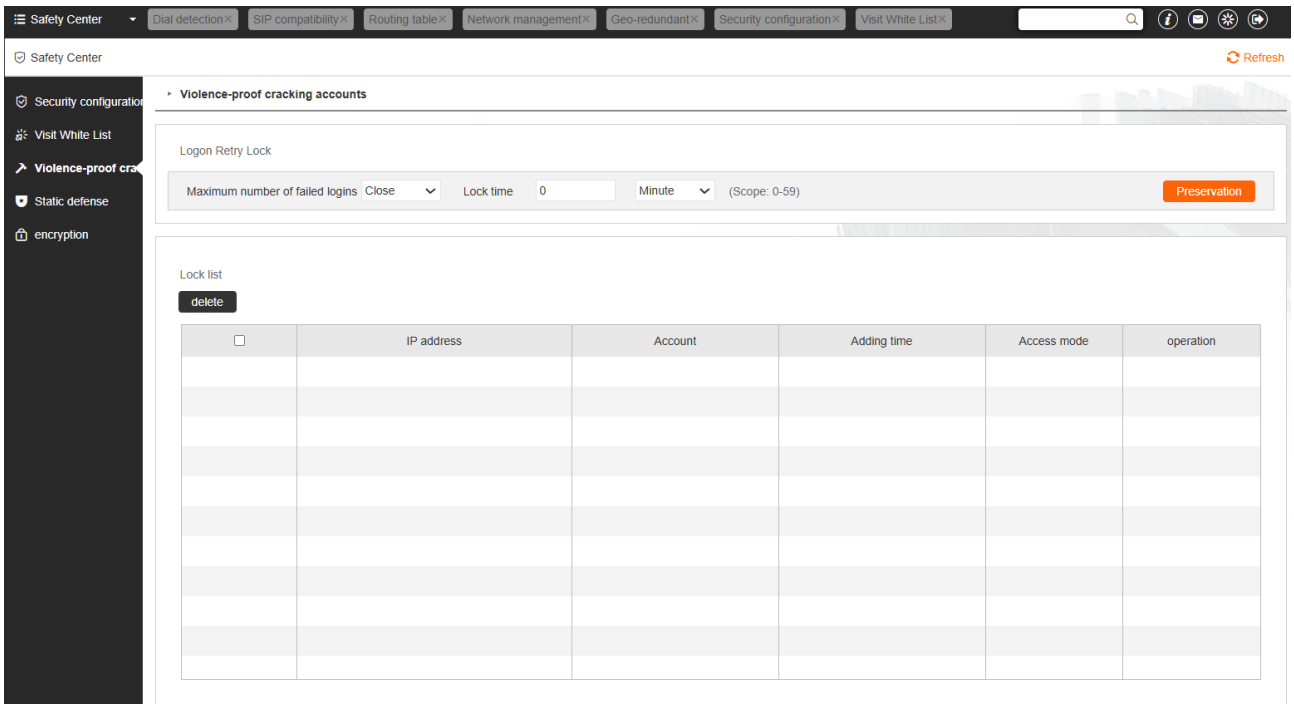


Table3.46 Anti-brute-force account break-in (login retry lockout) parameters

Item	Description
Maximum Number Of Failed Login Attempts	Configure the maximum number of failures allowed when accessing Web/SSH from the same IP address, beyond which a lockout list will be added. The configuration range is 1~6 times/day, and the default is 6 times/day.

Item	Description
Lock Duration	Configure the lockout time for the IP address. After locking for a sufficient length of time, the IP address will be unlocked, allowing access to the device again. The default is 10 minutes.

Locked list

The lock list is used to record the currently locked IP addresses.

Figure3-31 Anti-breakdown account (lock list) screen

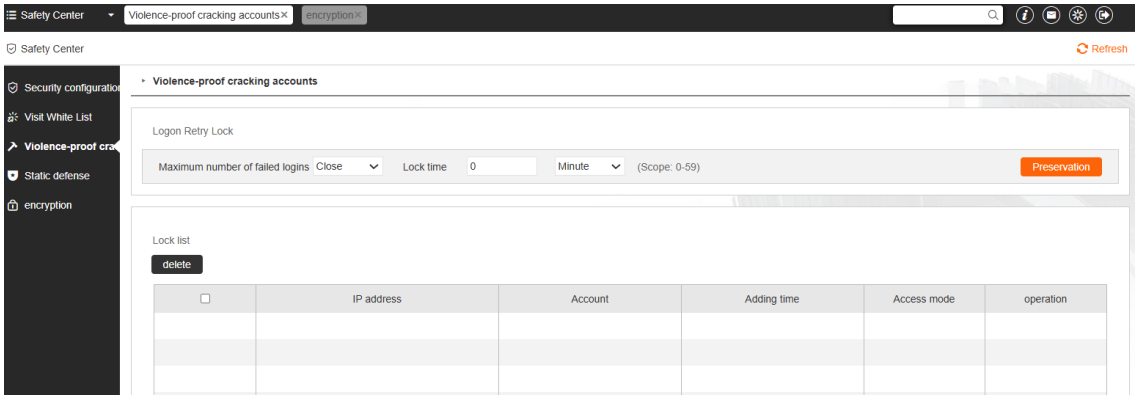


Table3.47 Anti-brute-force account (lockout list) display information

Item	Description
IP Address	Locked IP address
Add Time	Lock the time of this IP address
Access Method	How this IP address accesses the device (Web or SSH)

IP addresses are added automatically and cannot be added manually, only manual deletion is allowed.

- Delete :Deletes the selected entry. Deletion will unlock the IP address.

3.7.4 Static Defense

static defense

When the legality of certain IP addresses is known in advance, you can configure ACL-based traffic filtering rules to allow the reception of packets from legal IP addresses and prohibit the reception of packets from illegal IP addresses.

After logging in, clickSecurity Center>Static Defenseto open this configuration screen.

Figure3-32 Static Defense Configuration Interface

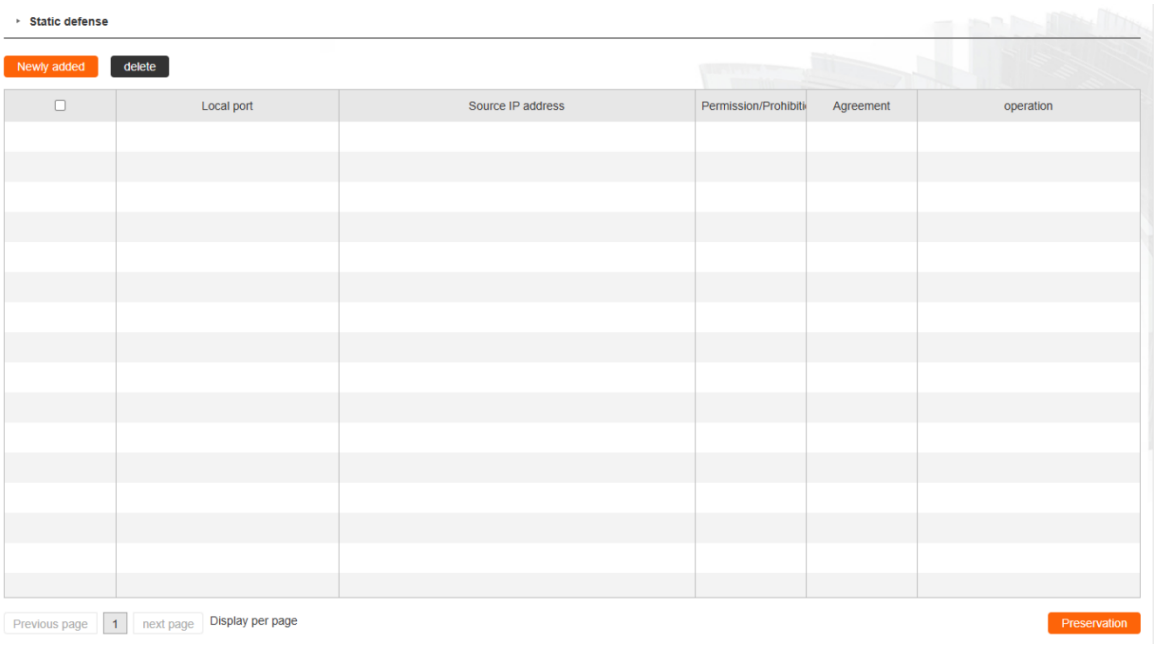


Table3.48 Static defense parameters

Item	Instructions
Local Port	Configure the local port range on which the device receives packets. The configurable port range is 0 to 65535.
Source IP Address	Configure the source IP address range. Note: Configuring domain names is not supported.
Allow/Prohibit	Configure whether to allow receiving packets from the source IP address when the rule matches.
Pact	Configure the protocol type, options include TCP, UDP, ICMP or any.

The following operations can be performed:

- New:Add a new rule.
- Copy :Copies the currently selected rule to the next one, making it easy to quickly add similar rules.
- Delete :Delete the current rule.
- Batch Delete: Delete the selected rules in batch.

Note

Static defense rules take effect in order from top to bottom.

 Copyright © Redstone Systems, Inc

2. typical example



The meaning of the example rule above is:

●Rule 1:Always allow port 80 of the device to receive TCP packets from the source IP address 192.168.120.54.

●Rule 2:Always disable the device's port 22 from receiving TCP packets from the source IP address 192.168.120.54.

● Rule 3:Always prohibit ports 5060 and 5061 of the device from receiving packets from the source IP address 192.168.120.54 (regardless of protocol type).

3.7.5 Encrypted

Go to Security Center>Encryptionto open this screen.

Figure3-33 Cryptographic Interface

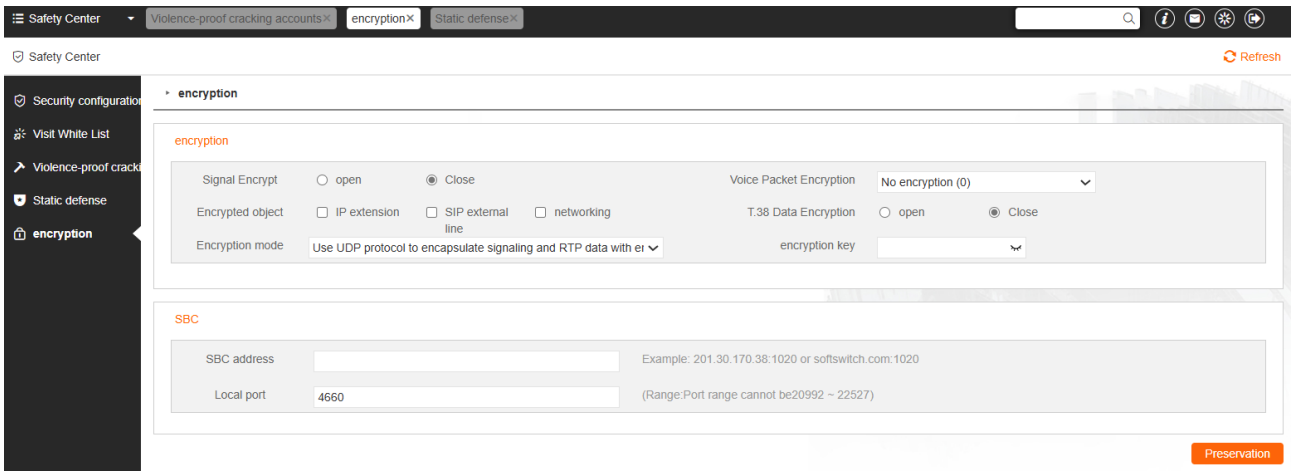


Table3.49 Description of encryption parameters

Item	Description
signaling encryption	Enables/disables signaling encryption. Default off.

Item	Description
Voice packet encryption	Select whether to encrypt RTP voice packets, default value 0. • 0: without encryption • 1: Encrypt all RTP • 2: Encrypts RTP packet headers only • 3: Encryption of RTP loads only
T38 Data Encryption	Select whether or not to encrypt T.38 fax media stream packets, the default value is not selected.
Encrypted Object	Select the encrypted object. • If you select IP extension or networking, you need the terminal to support encryption, otherwise the terminal will not work. • SIP outbound: choose whether to encrypt or not according to the needs of the SIP server.
Encryption Method	Sets the encryption method, the default value is 7. Optional parameters are: • Encapsulation of signaling and RTP data without encryption using TCP protocol (2) • Encapsulation of signaling and RTP data with encryption using TCP protocol (3) • Encapsulation of signaling and RTP data with encryption using UDP protocol (6) • Encapsulation of signaling and RTP data without encryption using the UDP protocol (7) • Using UDP protocol with RC4 encryption algorithm (10) • Special encryption in conjunction with Nanjing Kunshi VOS system (20) • Special encryption in conjunction with the Beijing Tianzhou communication system (21) The encryption method corresponding to different softswitch platforms can be selected as needed.
Encryption Key	from the operator or system administrator.
Sbc	When using the encryption method numbered (2) (3) (6) (7), it is necessary to use it with the Swift-Time SBC product.
SBC Address	Set the IP address and port number of the border proxy server. The address and port number are separated by ":". The proxy server address can be in the form of an IP address or in the form of a domain name, depending on the user's requirements. A complete and valid configuration is for example: 201.30.170.38:1020 or softswitch.com:1020. When using a domain name form of address, you need to configure a domain name resolution server in theBasic Configuration > Networkinterface. For example: 201.30.170.38:1020 or softswitch.com:1020.

Item	Description
Local Port	The value of the local port on which the device interfaces with the border proxy server, the default value is 4660. The local port value can be set arbitrarily, but cannot conflict with other port numbers used by the device, such as 5060.
VOS Encryption Key	When using the Nanjing Kunshi VOS system encryption method numbered (20), you need to fill in the corresponding user name and password.
User ID	VOS encryption key username.
Cryptographic	VOS encryption key password.

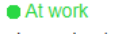
3.8 System Maintenance

3.8.1 Board Management

Board management is used for the daily maintenance of each board. The interface displays the status of each card on the panel in real time.

Go toSystem Maintenance>Board Management to view it.

Table3.50 Description of Board Management

State Of Affairs	Instructions
Normalcy	No board abnormality
Loss	The board is connected incorrectly, or the board does not exist. After performing the confirmation, the board shows unplugged.
Additional	Newly insert the board, make a confirmation, and the board enters the normal working state.
Deactivate	Board is deactivated
Malfunctions	Board failure
Unplugged	When the board is displayed as missing, after clicking Confirm, the board appears blank, indicating that the board is not plugged in.
At Work	When dual stacking, it indicates that the current chassis is the host. 
Pending	When dual-stacking, the chassis that is not labeled "active" is the standby.
Buttons	Description
Startup, Restart, Deactivation	Check the checkbox in front of the board, and then click the button to start, disable, and reboot the board.

 Copyright © Redstone Systems, Inc

3.8.2 System expansion

For new chassis with expansion, you need to confirm the hardware to see if it is properly connected and installed before configuring the network.

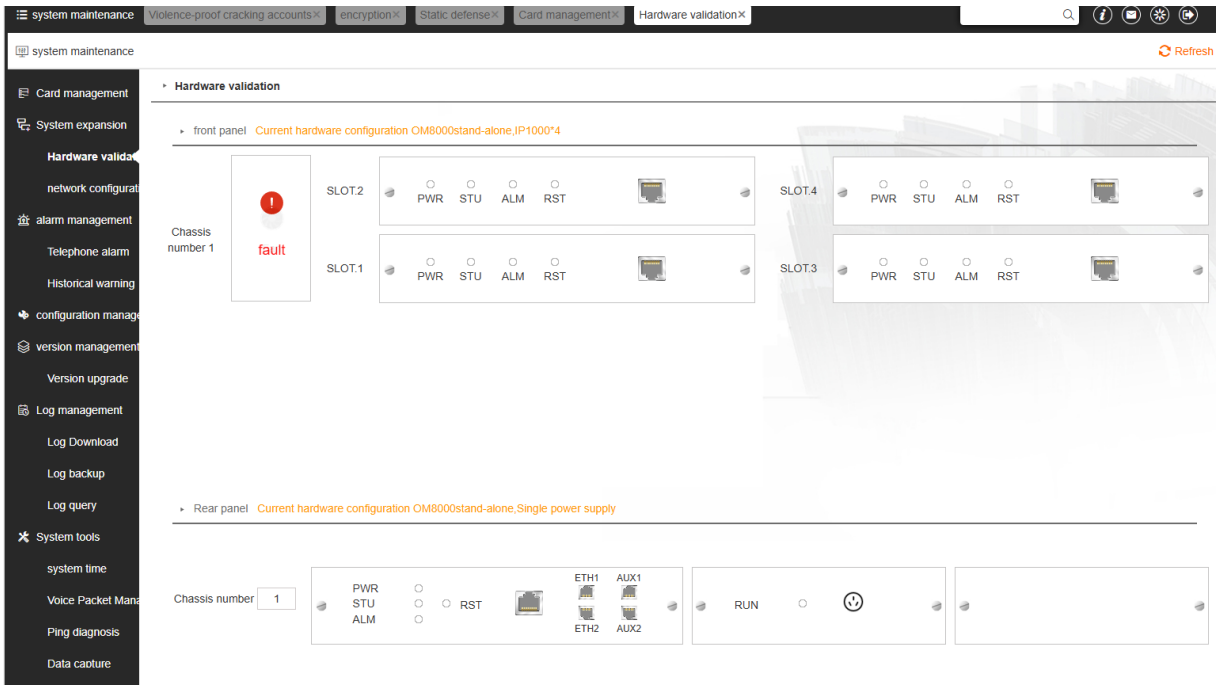
Step1. Hardware Confirmation

Go to System Maintenance>System Expansion>Hardware Confirmation.

This page displays the current device's hardware such as host, daughter card, power supply, and fan. If the display does not match the expectations of the purchase, check the device connection.

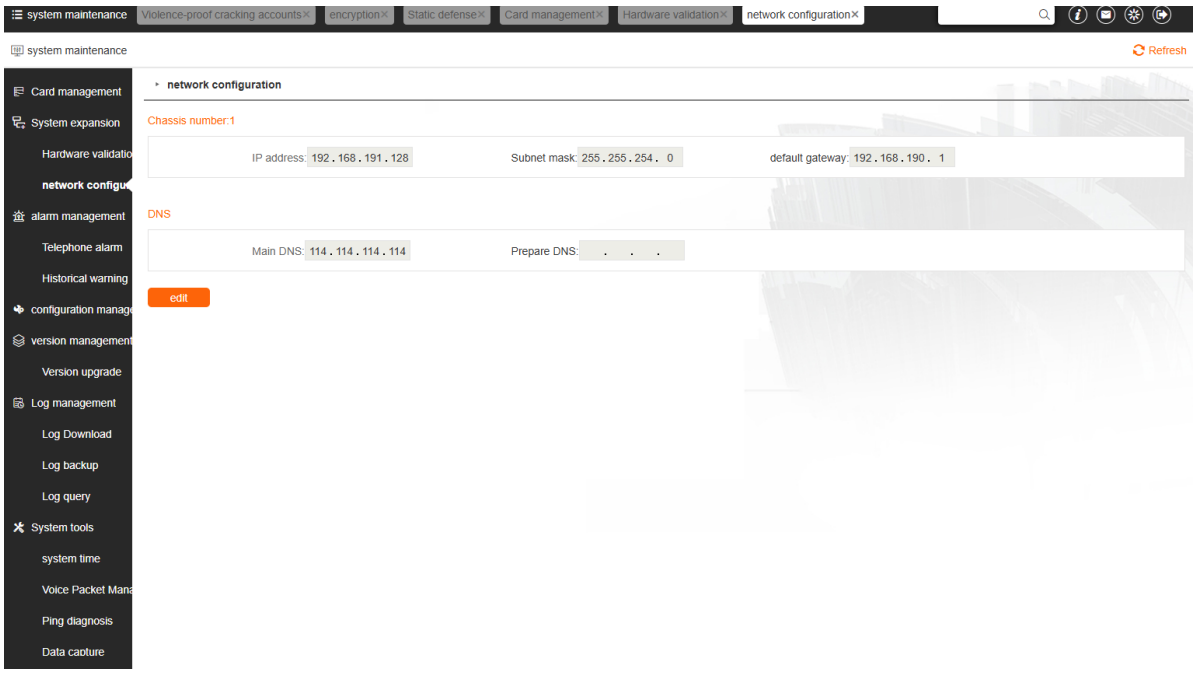
When the new chassis is connected properly, the system will detect it and prompt "New machine found" on the page.

Follow the prompts to complete the hardware board confirmation and chassis number selection.



Step2. network setup

Go to System Maintenance>Network Configuration>Editto configure the network parameters for the added chassis and the entire machine.

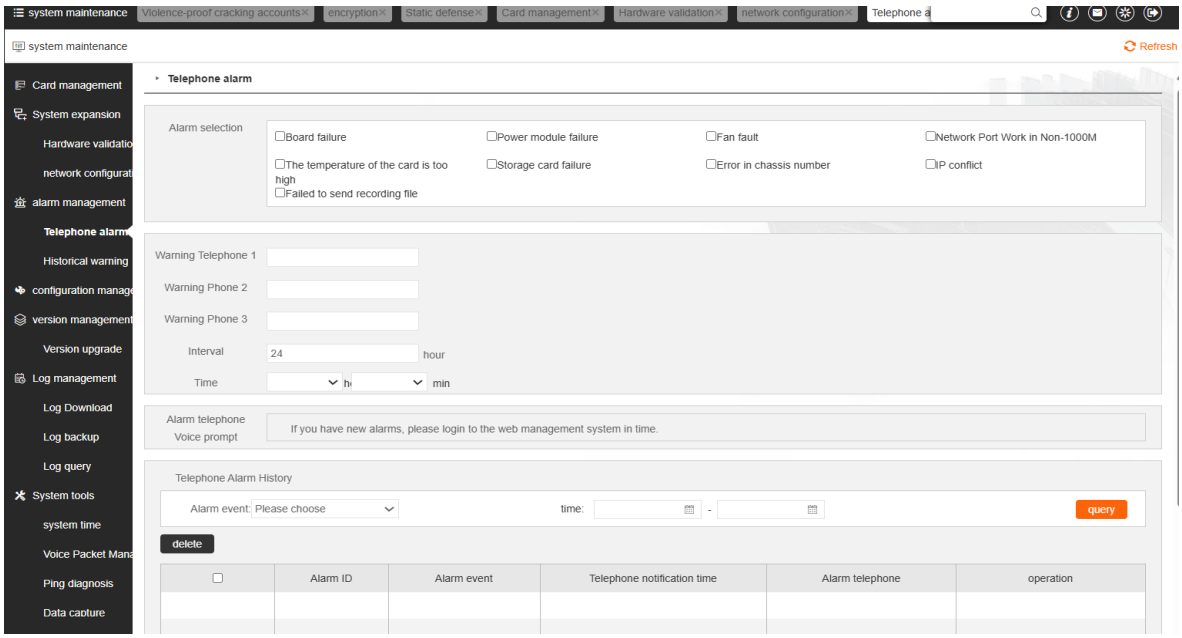


3.8.3 Alarm Management

Telephone alarm

Go to theSystem Maintenance > Phone Alarmspage to configure the phone number and phone alarm category to answer the alarm.

 Copyright © Redstone Systems, Inc



Alarm History

Go to theSystem Maintenance > Historical Alarmspage to view historical alarm information and to acknowledge and eliminate alarms.

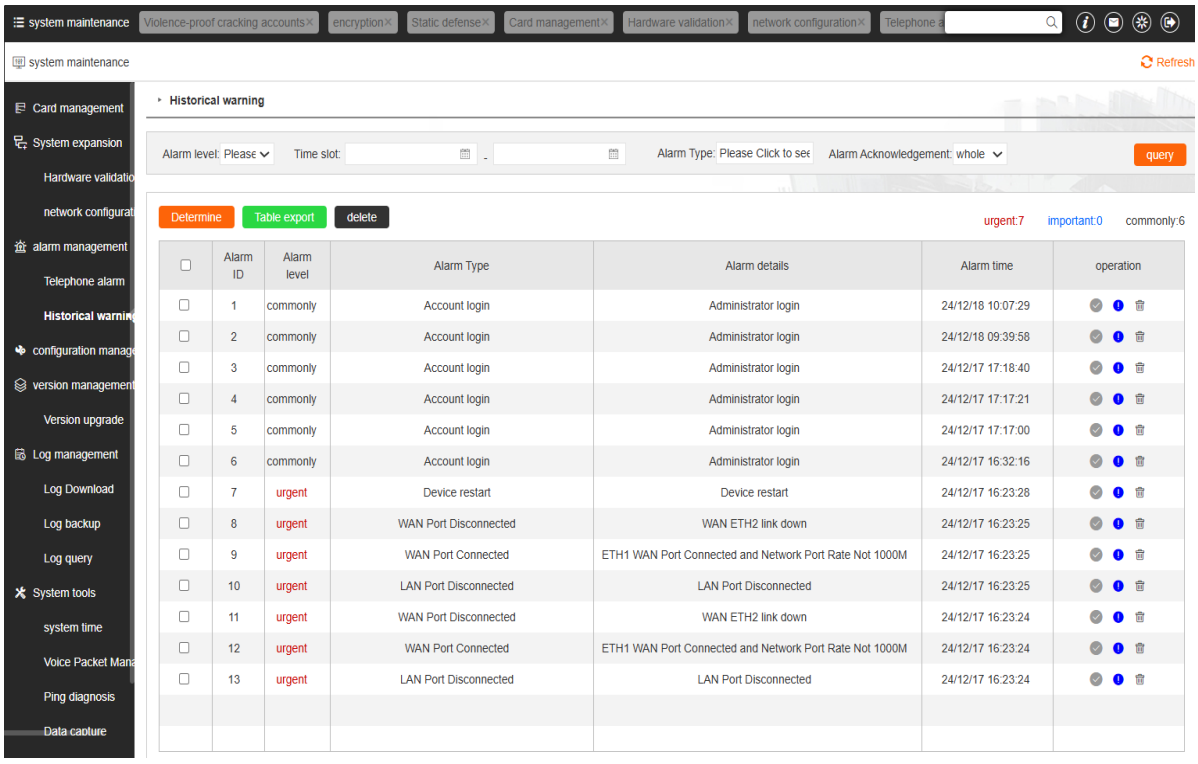


Table3.51 Classification of alarm messages

Form	Element
general	IP Outside Line Registration Successful
	IP outbound registration failure
	Modify the SIP port
	WAN connected
	Operator Login
	Administrator Login
	IP address change
	Board Failure Recovery
	Chassis operating temperature recovery
	Primary and secondary SIP server switchover recovery
	Recording Failure Recovery
	CPU overload recovery
	Memory Overload Recovery
	New card detected
	Discover the new REX8000 host
	Discover new IP1000 boards
	The network operates in non-full-duplex mode
	Network working in non-full-duplex mode recovery
Important Alerts	Change administrator password
	Wrong login password
	Change operator password
	be subjected to a SIP attack
	Concurrent calls too high
	Port redundancy
	Failed to send recording
	CPU overload
	memory overload
	Memory card limitations
	Excessive international calling hours
	SSH enabled
	SSH login
	Change SSH password
	SSH login password error
	restore the factory
emergency alert	Device reboot

 Copyright © Redstone Systems, Inc

Form	Element
	software restart
	board failure
	Veneer Reboot
	DNS resolution failure
	single-unit failure
	Power module failure
	Fan failure
	The network port works on non-1000M
	High chassis operating temperature
	Board temperature too high
	Switching between master and backup
	Memory card failure
	dual-unit conflict
	Chassis number not recognized
	Dual-computer cascade not connected
	IP conflict

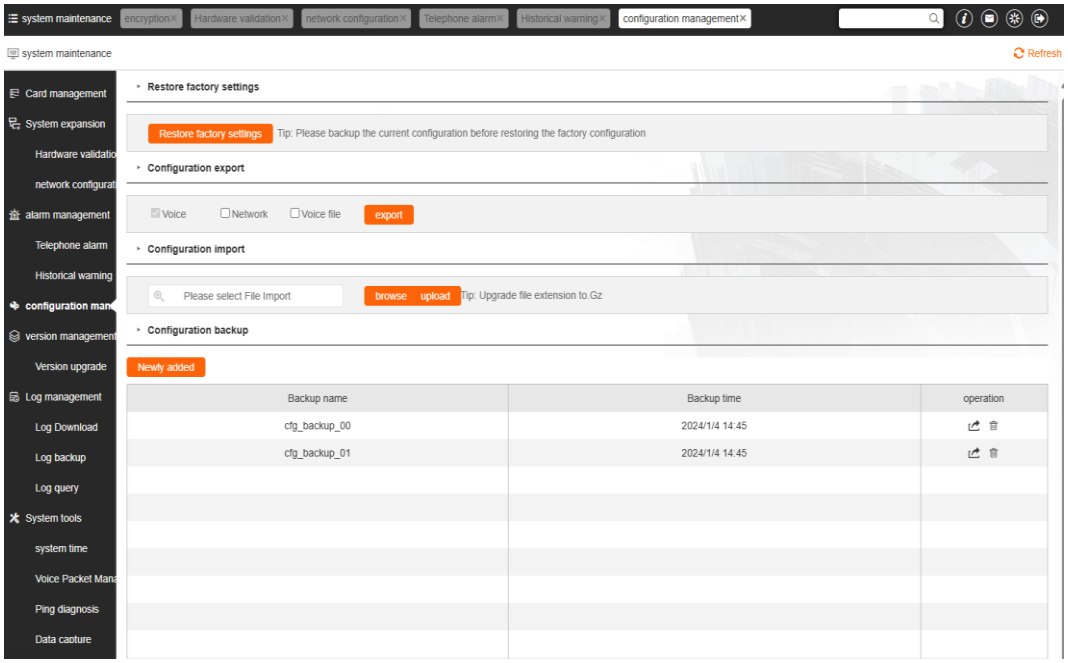
3.8.4 Configuration Management

Go to System Maintenance>Configuration Managementto import, export, backup device configuration and restore factory settings.

Before restoring the factory configuration, it is recommended to take a configuration backup by clicking New at Configuration Backup.

The imported configuration package is displayed in the "Configuration Backup" list, click  and then click OK, the device will be restored to this configuration package, and the configuration is imported successfully.

 Copyright © Redstone Systems, Inc



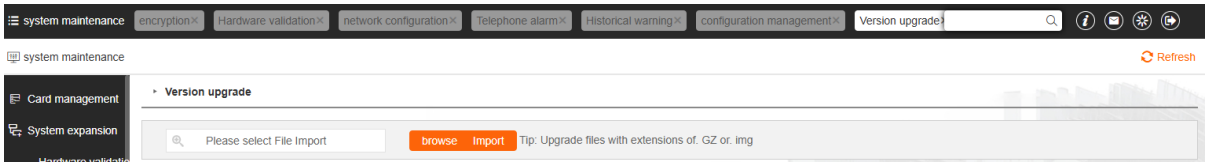
Note

- Supports exporting network configuration, SIP&PBX configuration, and voice files in the system respectively, and only SIP&PBX configuration is exported by default.
- The speed of importing and exporting configuration files is affected by the network, so please be patient.

3.8.5 Version Management

Go to System Tools>Version Management>Software Upgrade, import the upgrade package file, and follow the prompts to perform the upgrade operation.

Figure3-34 Software Upgrade Screen



Allow version rollback.

Note

- The upgrade will take about a few minutes, so please do not do it during peak call times.
- Do not power off, disconnect, or reboot the device during the upgrade period, as this may result in system corruption and failure to boot the device. After the upgrade is successful, the device will reboot automatically.

3.8.6 Log Management

Log Download

Go to System Maintenance>Log Management>Log Download.

Logs record information about changes in device status during operation and can be used to locate device failures and understand network conditions.

Select the board and chassis that you need to view the days, select the log level, and clickDownloadto download the logs.

Figure3-35 Log Download Screen

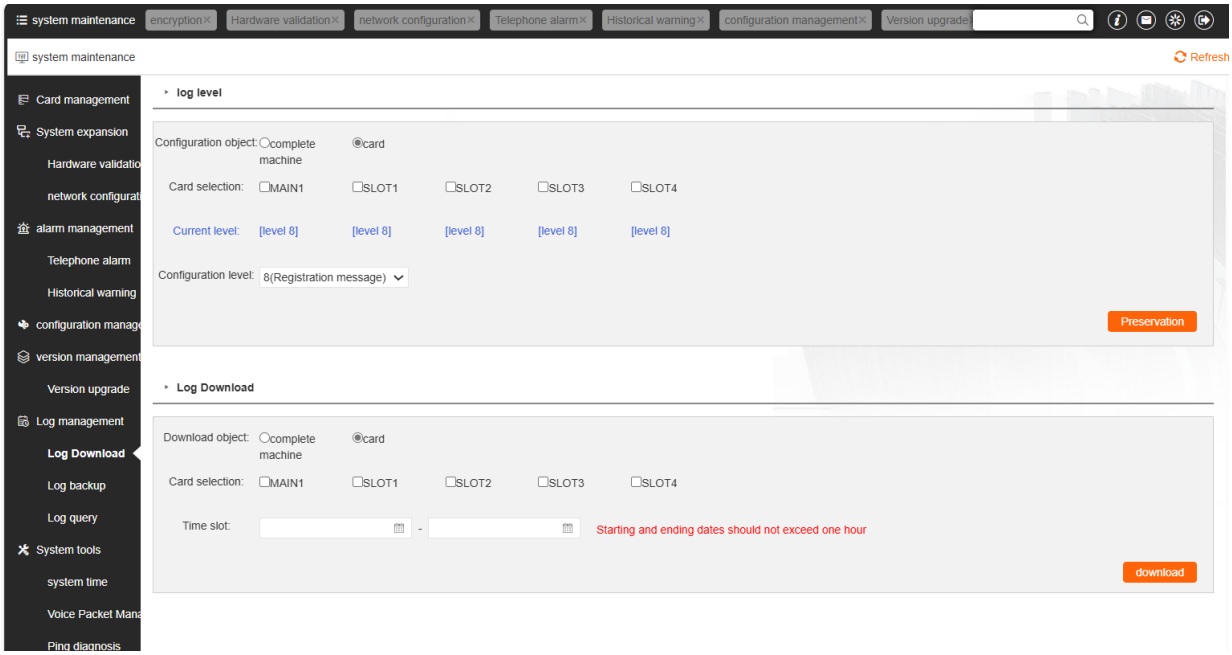


Table3.52 Log Download

Item	Description
Log level	
Configuration objects	Whole machine: i.e., level setting for the overall log of the device Board: You can select the corresponding board for which you want to set the logging level.
Board Selection	SLOT1~8 (representing 8 daughter cards for dual machines respectively)
Configuration level (level)	Select the level of logs to be downloaded Note: Each time the device reboots, it will restore the syslog level to the default.

 Copyright © Redstone Systems, Inc

Item	Description
Logbook Download	
Download objects	Whole machine: i.e. download the whole log of the device Board: You can select the corresponding board to which you want to download logs.
Board Selection	SLOT1~8 (representing 8 daughter cards for dual machines respectively)
time period	Download log messages generated during this time period
Number Tracking	
Extension Number Tracking Outside Number Tracking	Log tracking for a particular extension or outside line, with a 7-day tracking limit

Table3.53 Log Backup

Go toSystemMaintenance>LogManagement>Log Backup, set the FTP server address and user name and password, and the logs will be backed up automatically.

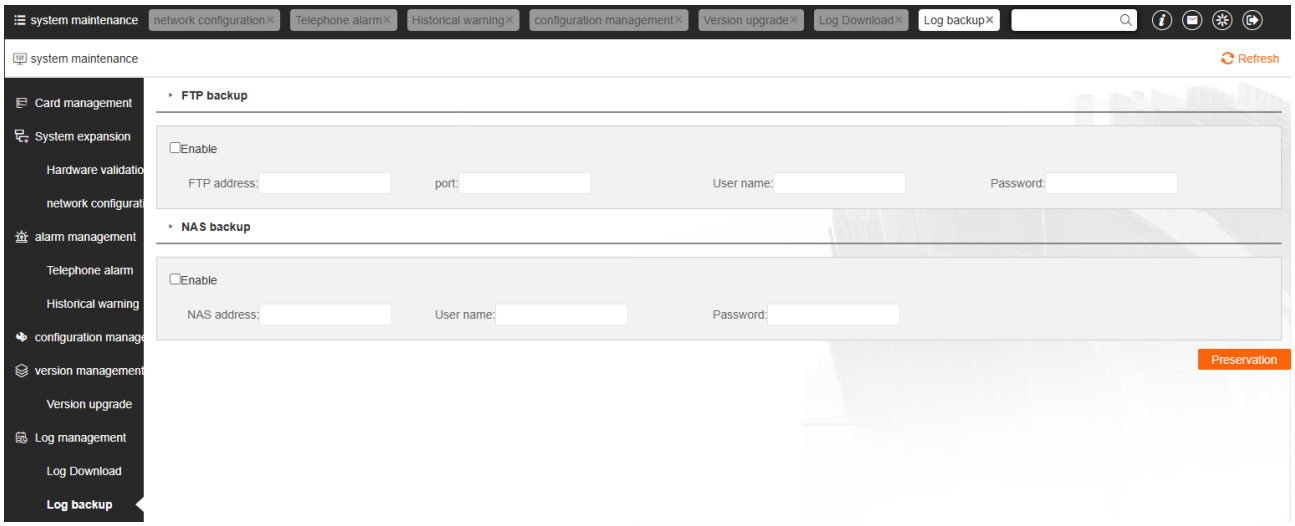


Table3.54 Log Backup

Item	Description
FTP Backup	The logs backed up to the FTP server can be viewed under the specified path of the FTP server, which is "Folder named by the device MAC address\subfolders with different dates\subfolders with different boards", for example, D:\FTP\000EA966000B\20190523\22. Logs do not include viewing the day's log.
FTP address	Fill in the address of the FTP server
ports	Fill in the port of the FTP server, default 21
user ID	Fill in the user name set up on the FTP server

 Copyright © Redstone Systems, Inc

Item	Description
cryptographic	Fill in the password set on the FTP server

3.8.7 System Tools

System Time

The system time of the device can be obtained by synchronizing with a time server in the network. The device has a clock function with a battery that keeps it running when the device is powered off.

ClickSystem Maintenance > System Time to configure the time server.

Figure3-36 System Time Configuration Screen

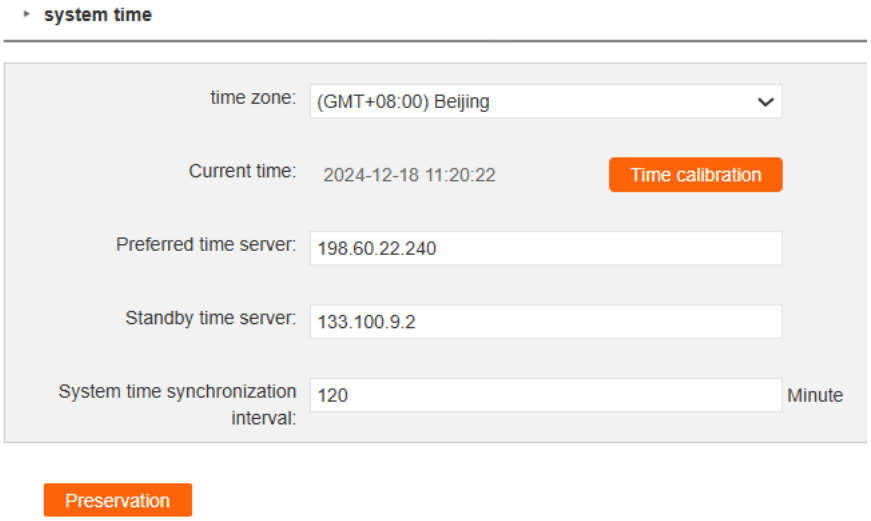


Table3.55 Description of system time parameters

Item	instructions
time zones	Select the time zone according to the region where the device is located.
current time	Displays the current time of the device, and you can clickClock Calibrationto calibrate the time.
Preferred Time Servers	Enter the preferred time server IP address here. There is no default value for this item.
backup time server	Enter the alternate time server IP address here. There is no default value for this item.

 Copyright © Redstone Systems, Inc

Item	instructions
System time synchronization interval	The period in minutes for the device to synchronize with the network time server, the default is 120 minutes.

Note

If you cannot synchronize with the time server, you can click theClock Calibrationbutton to set the PC's time to the system time.

Voice packet management

Each voice pack corresponds to one language and contains all system voice prompt files. For details, seeTable3.56.

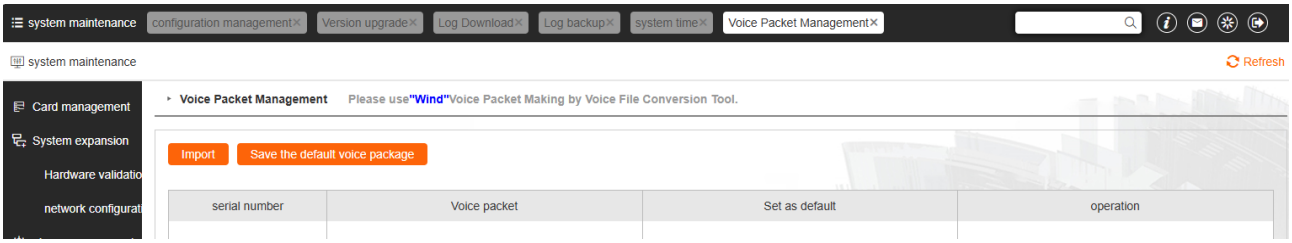
The following steps describe uploading a pre-recorded voice packet to the device.

Step1. Click System Maintenance>Language Pack Managementto enter the configuration interface.

Step2. Click Importto import a pre-made voice pack.

Step3. Click the Set as Default check box and then click Save Default Voice Packto set the system default voice pack.

Figure3-37 Voice Pack Configuration Interface



Step4. Click the voice pack corresponding to , you can view the individual voice files. Replacement individual voice files can be uploaded if needed.

Table3.56 System voice prompt file

Filename	Element
0_tip	(placed between two numbers indicate a smaller quantity followed by a larger one)
1_tip	"one" radical in Chinese characters (Kangxi radical 1)
2_tip	stupid (Beijing dialect)
3_tip	surname San
4_tip	4
5_tip	5
6_tip	6
7_tip	7

 Copyright © Redstone Systems, Inc

Filename	Element
8_tip	8
9_tip	9
account	Please enter your password.
block	You do not have enough call privileges, please contact an administrator.
busy	Sorry, the extension is busy, please dial another extension number, or the switchboard will serve you later.
callwaiting	The extension is on the line, please do not hang up.
connect	Transferring, please wait.
disable	Close.
dnd	The user you are calling has the Do Not Disturb feature enabled, please hang up.
dot_tip	Point.
enable	Open.
gateway	Gateway Address.
groupbusy	Extensions are busy, please be patient.
hangup	I'm sorry, the call will be disconnected. Please call again. Goodbye.
hangup2	The call will hang up in one minute.
ip_tip	The local network address.
IVR1	To set Call Forwarding press 1, to set Voice Message press 2, to set Do Not Disturb press 3, to set Simultaneous Ovation press 4, to set Call Waiting press 5, to set Color Ringing press 6, to set other extensions press 7, to answer again press 9.
IVR2	Please enter the extension number plus the code, ending with the # key.
IVR3	This feature is not available, please contact the administrator.
IVR4	To get the current configuration press the * key, to return to the upper menu press the # key.
IVR5	Business registration was successful.
confirm	Business registration was successful.
IVR6	Business registration failed.
wrong	Business registration failed.
IVR7	Business canceled successfully.
cancel	Business canceled successfully.
IVR8	The password you have entered is incorrect, please re-enter it.
reenter	The password you have entered is incorrect, please re-enter it.
IVR9	Current Settings.
setting	Current Settings.
IVR10	To activate Do Not Disturb press 1, to deactivate press 0.
IVR11	Press 0 to close the message, press 1 to transfer the message for all incoming calls, and press 2 to transfer the message when the call is not answered.

 Copyright © Redstone Systems, Inc

Filename	Element
IVR12	To listen to the current ringtone, press *, to change the ringtone, press 2, to close the ringtone, press 0, and to return to the upper menu, press #.
IVR14	To set the number, press 1.
IVR14A	Press 0 to turn off resonance and 1 to turn on and configure the resonance number.
IVR15	Please enter the number, ending with the # key.
IVR16	To turn off Call Forwarding press 0, to set the Call Forwarding number press 9, to turn on Unconditional Forwarding press 1, to turn on Busy or No Answer Forwarding press 2, to get the current configuration press the * key, and to return to the parent menu press the # key.
IVR18	The password you have entered is incorrect, please re-enter it.
netmask	Subnet Mask.
noanswer	Sorry, the call was not answered, please dial another extension number or dial 0 to be served by the switchboard.
nocircuit	There are currently no available outbound lines, please try again later.
nonumber	Sorry, the number you have dialed is empty, please re-enter it. To check the number, please dial 0.
offhour	We welcome your call. It's after hours, so please dial the extension number directly.
operator	Please wait a moment while the switchboard serves you.
operbusy	Sorry, the switchboard is busy. To continue waiting, please press the * key, or dial another extension instead.
port	Line number.
record	Please start recording after the beep, and hang up when finished.
tryagain	The number you have dialed cannot be reached at the moment, please dial again later.
version	Software Version.
vm_all	Your call will be forwarded to voicemail, please leave a message after the beep and hang up when you have finished.
vm_busy	Extension is in the middle of a call, please leave a message after the beep, please hang up after the message is finished.
vm_fail	The extension is temporarily unavailable, please leave a message after the beep, please hang up after the message.
vm_noans	If your extension is not answered, please leave a message after the beep and hang up when you have finished.
webport	Manage ports.
welcome	Welcome to your call, please dial the extension number directly, and dial 0 for number checking.
vm_new	___ new voice messages
vm_no	You have no voice mail.
vm_old	___ old voice messages

 Copyright © Redstone Systems, Inc

Filename	Element
vm_pre	You have ___
vm_prompt	Press 1 to relisten to the voice message, press 2 to delete, and press 3 to listen to the next message.
wakeup	Hello, this is the wake-up call service, your wake-up call time has expired, hope to serve you again.
btime	Sorry, the current time is not allowed to call, please contact the administrator if you need to adjust it
binternal	Sorry, your current calling privilege is an extension, if you need to adjust, please contact the administrator
lock	Sorry, your extension is locked. Please unlock it first.
bres	Sorry, the system doesn't allow you to call this number
bdomestic	Sorry, your current calling privilege is domestic long distance, if you need to adjust, please contact the administrator
blocal	Sorry, your current calling privileges are for local calls, please contact the administrator if you need to adjust them

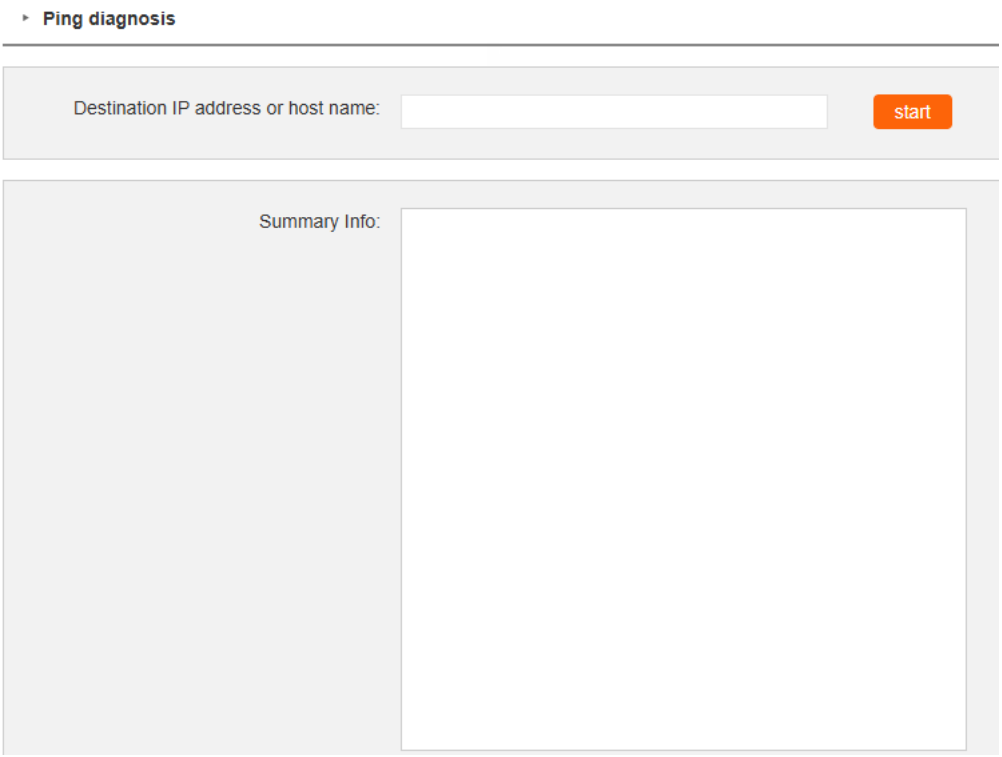
Ping Diagnostics

This tool is used to diagnose whether the network is connected or not.

Go to System Maintenance>Ping Diagnosticsand fill in the destination IP address or host name to start the diagnostics. Diagnostics can be viewed in theSummary Informationbox.

Figure3-38 Ping Diagnostic Interface

 Copyright © Redstone Systems, Inc



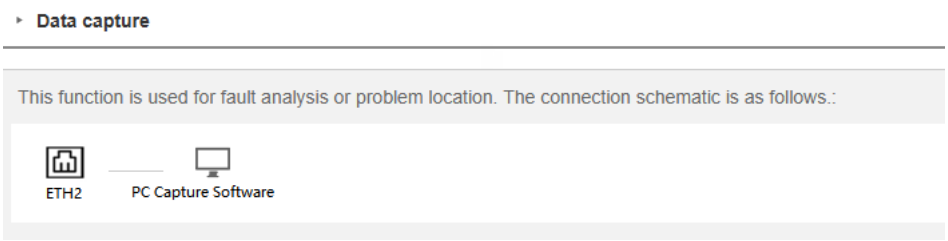
Packetization

Data Capture is the real-time saving of Voice over IP packets in the device. When there is a problem involving IP voice double pass, single pass, murmur, echo, etc. in the device, the data capture function helps to analyze and locate the problem, and the stored packets are temporarily stored in the device in the form of dump.cap file packets.

Go toSystem Maintenance>System Tools>Data Capture.

- When both ETH ports of the device are already in use (redundant mode or IMS leased line access mode)

2. PC Connection Mirror Switch
3. Enable mirroring capture in the REX8000 interface
4. The PC opens packet capture software (e.g. Wireshark) to capture packets



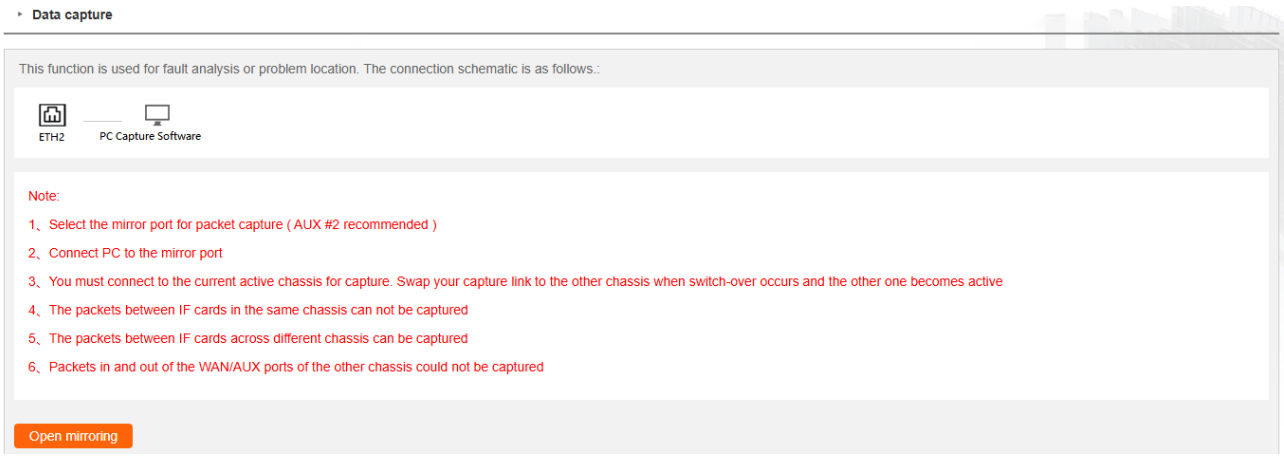
- When the device is in switching mode

1. PC configured with static address 169.254.0.18, directly connected to the device's free

ETH port

2. REX8000 Interface Enables Packet Grabbing

3. The PC opens packet capture software (e.g. Wireshark) to capture packets



Delegation Management

Some features of the device require a License authorization file to activate or expand capabilities.

When the License authorization file is not imported, the factory default maximum number of extensions is 1000, and the maximum number of SIP outside lines is 1000.

Go to System Maintenance>SystemTools>License Management(the menu is pulled to the bottom) and import the License file.

 Copyright © Redstone Systems, Inc

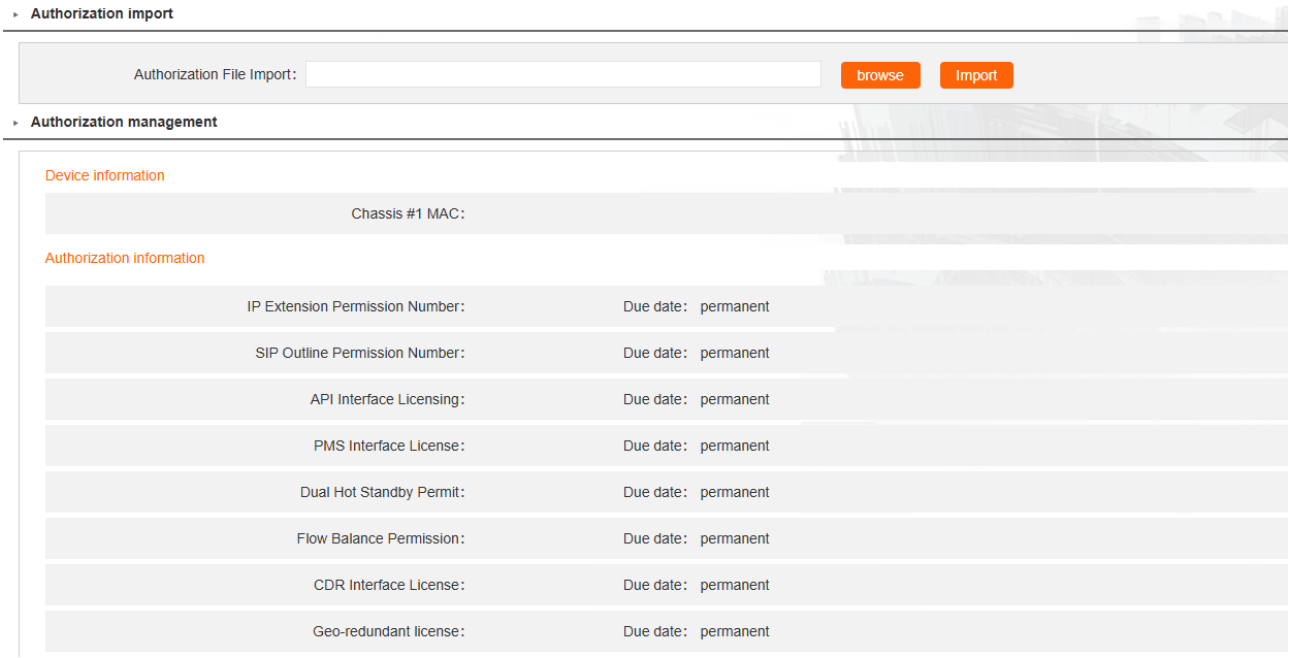


Table3.57 Authorization Management Parameters

Item	Description
Authorization file import	The imported license file extension must be lic. Only one license can be imported at a time, if you need to import more than one, then import one first, refresh and then import, no order required.
Equipment Information	Manufacturer production authorization file production before the need to obtain the device's MAC address (very important). Except for the License for dual hot standby, which requires obtaining the MAC addresses of both chassis, only the MAC address of chassis 1 is required in other cases.
Number of IP extension licenses	Maximum number of supported extensions, factory default is 1000 when there is no License file.
SIP outbound license	Maximum number of supported SIP outside lines, factory default is 1000 when no License file.
API license	Activate: allow use of API interface Not activated: API interfaces are not permitted
PMS interface license	Activation: PMS interface allowed Inactivated: PMS interface not allowed
dual hot standby license	Activate: Enable the dual-machine hot standby function. That is, when the main control card of one chassis fails in the dual-computer state, it will automatically switch to the main control card of the standby chassis, which will have no impact on the business. Inactivated: the Dual Hot Standby feature is not allowed.

 Copyright © Redstone Systems, Inc

Item	Description
Traffic Balancing License	Number of supported traffic balancing resource boards (2 to 8). When a resource card within the license number fails, the device automatically balances the services that should be burdened by this card to other resource cards within the license number.
CDR interface license	Activation: CDR interface allowed Not activated: CDR interface not allowed

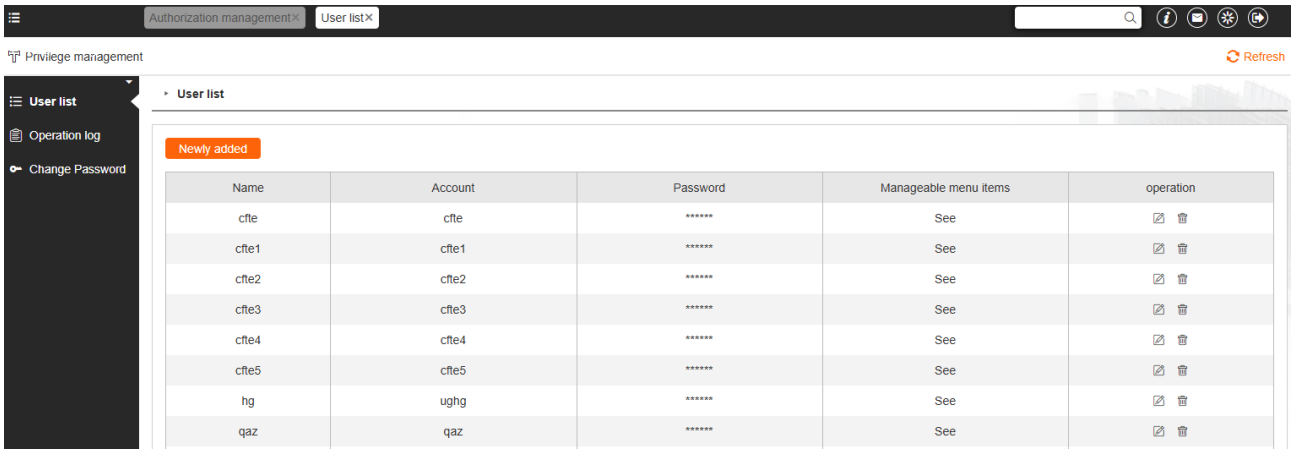
3.9 Rights Management

3.9.1 User List

The system default admin super administrator can create 10 new ordinary administrators and assign them different operation privileges for different pages. Flexible page permission management for customers.

The same administrator and regular administrator can only log in on one PC at the same time.

Step1. Go to Permission Management>User List.



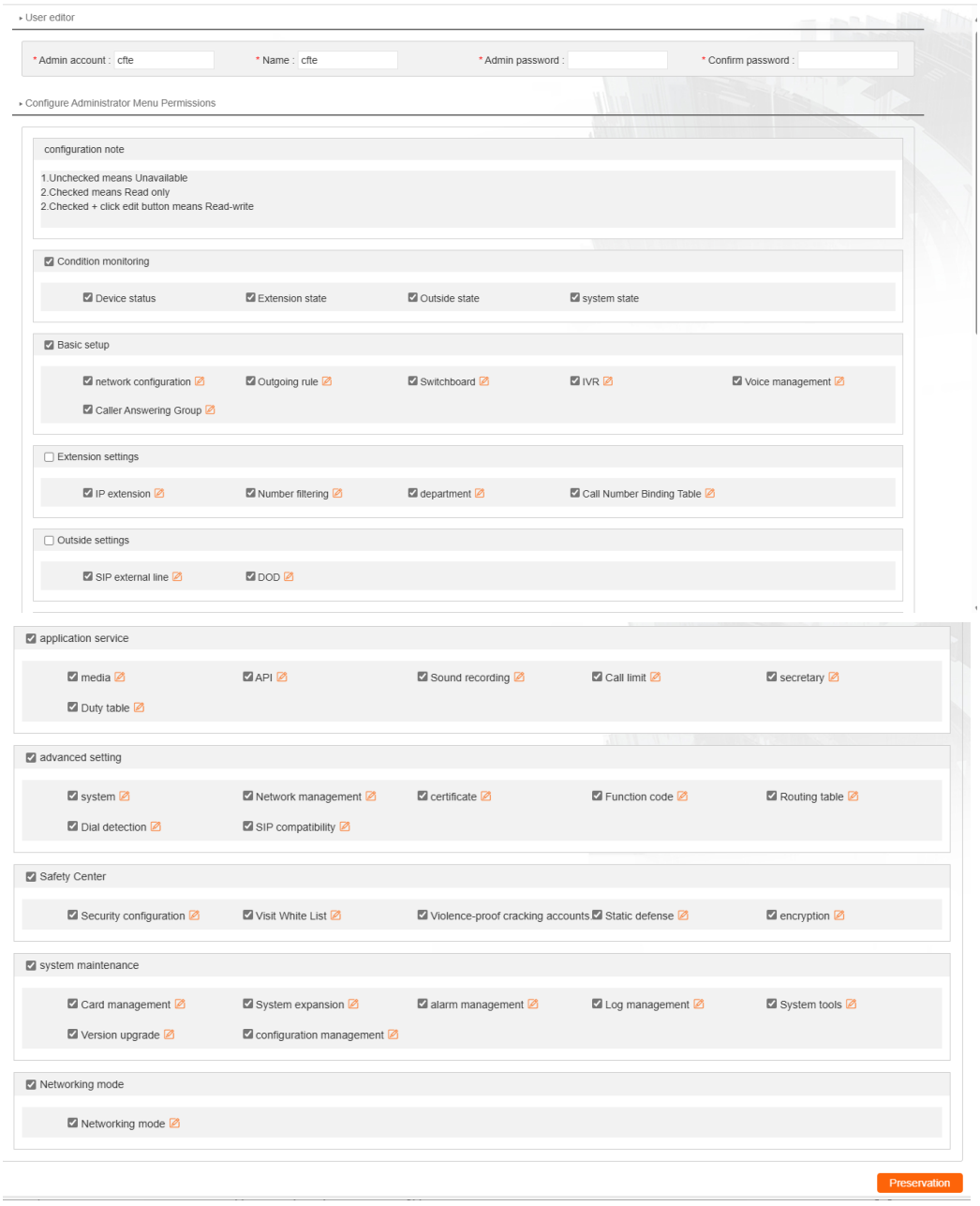
Step2. Click New to create a new administrator account and specify the operating privileges for that account.

There are three types of operating privileges, including:

- Unchecked means "unreadable and unwritable".

- Checked for "readable".
- Checking the box and clicking the edit button means that it is "readable and writable".

Step3. ClickSave.



3.9.2 Operating Log

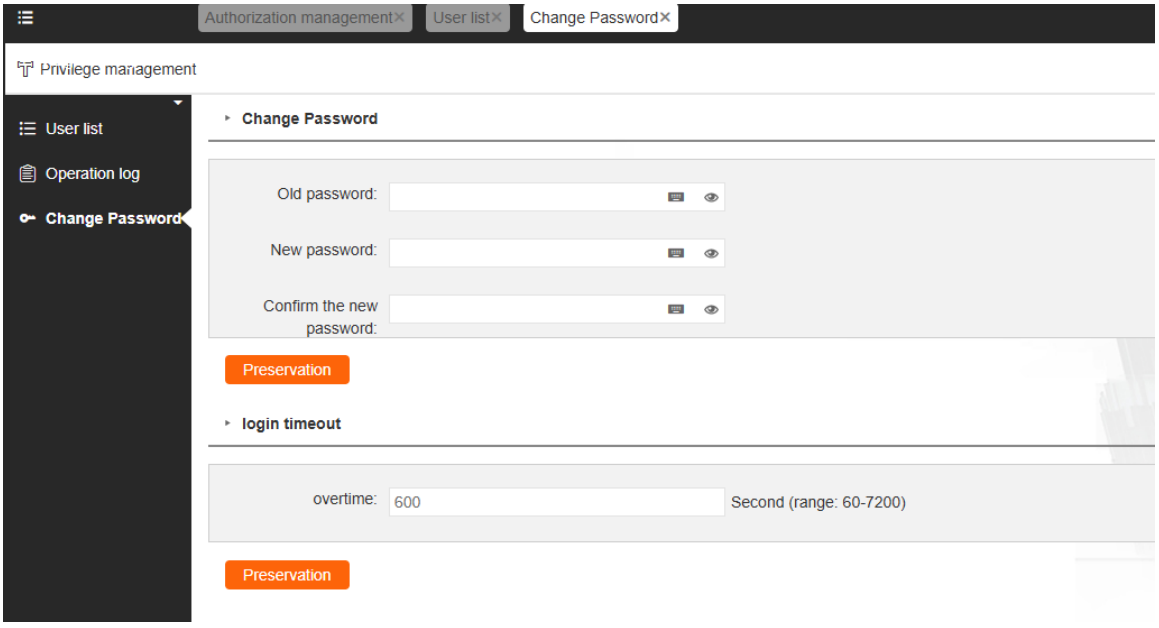
Modifying configurations and creating, deleting, and modifying users generates operation logs.

Go to Permission Management>Operation Logto query or export the operation log of the specified administrator account. The exported action log is saved as userActionLog.xlsx file.

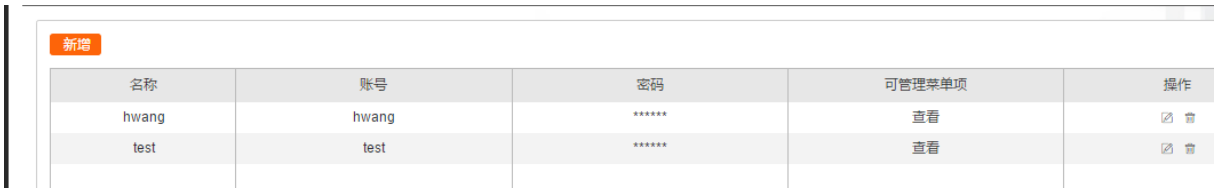


3.9.3 Modify A Password

Modify administrator password: Go toPermission Management>Modify Password, modify it and clickSave.



Change the general admin password: Go to Permission Management>User Listand click to change the password. ClickSave.



3.10 Network Setup

Networking is the process of connecting multiple devices to each other over an IP network, thereby realizing short extension dialing and outside line sharing between devices.

The extension number of the equipment in the network is unique, and when the extensions in the network dial each other, you can dial each other's extension number directly.

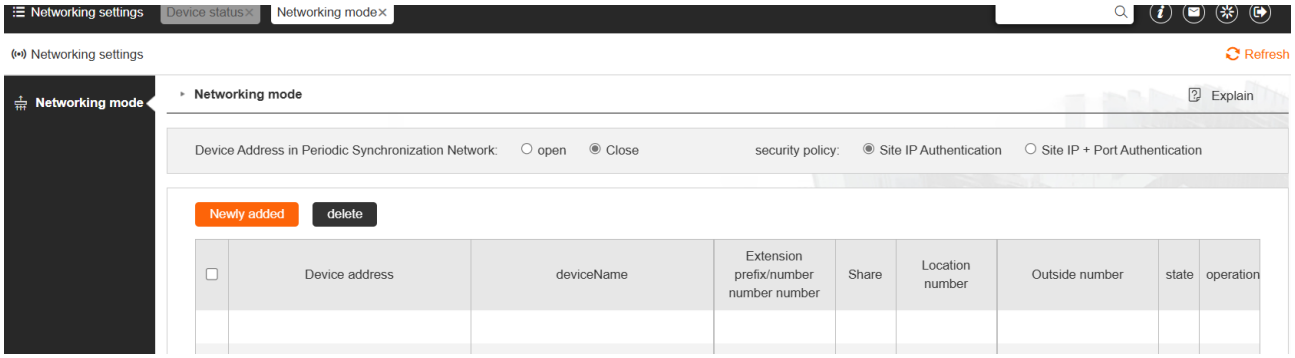
Deployment requires uniform planning of the extension numbers of all devices in the network to avoid number conflicts.

When configured, the first device in the grouping list is the management site, which is responsible for obtaining updates from each site and publishing them to each common site. Each common site only needs to configure the management site and its own information, so that it can periodically get information about other sites from the management site.

Managing the site

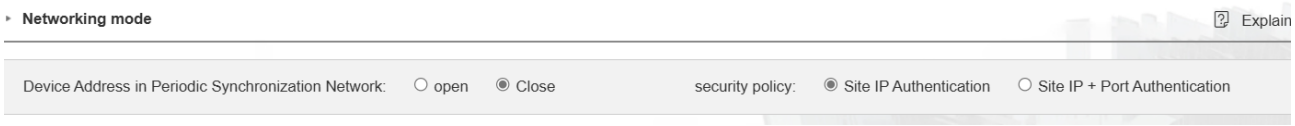
Step1. Go toNetworking Settings>Networking Methods.

Figure3-39 network interface



Step2. Enable periodic synchronization of device addresses on the network.

Figure3-40 Network Configuration Interface



Step3. Select the security policy. the OM provides two authentication methods.

Table3.58 Security Policy Parameters

Item	Description
Site IP Authentication	Authentication site device IP address. If the IP address of the message sender matches the settings in the network list, it is considered to be a trusted device, and the message sent from it is processed. When other devices in the network are located in the private network, after NAT, which may result in unfixed ports, this device selects site authentication.
Site IP + Port Authentication	Authentication site IP address and SIP port number. Both the IP address and SIP port number of the message sender need to match the settings in the networking list to be considered a trusted device. Otherwise received messages are ignored.

Step4. Adding a management site

ClickNewand enter the management site information.

Figure3-41 Add Site Screen

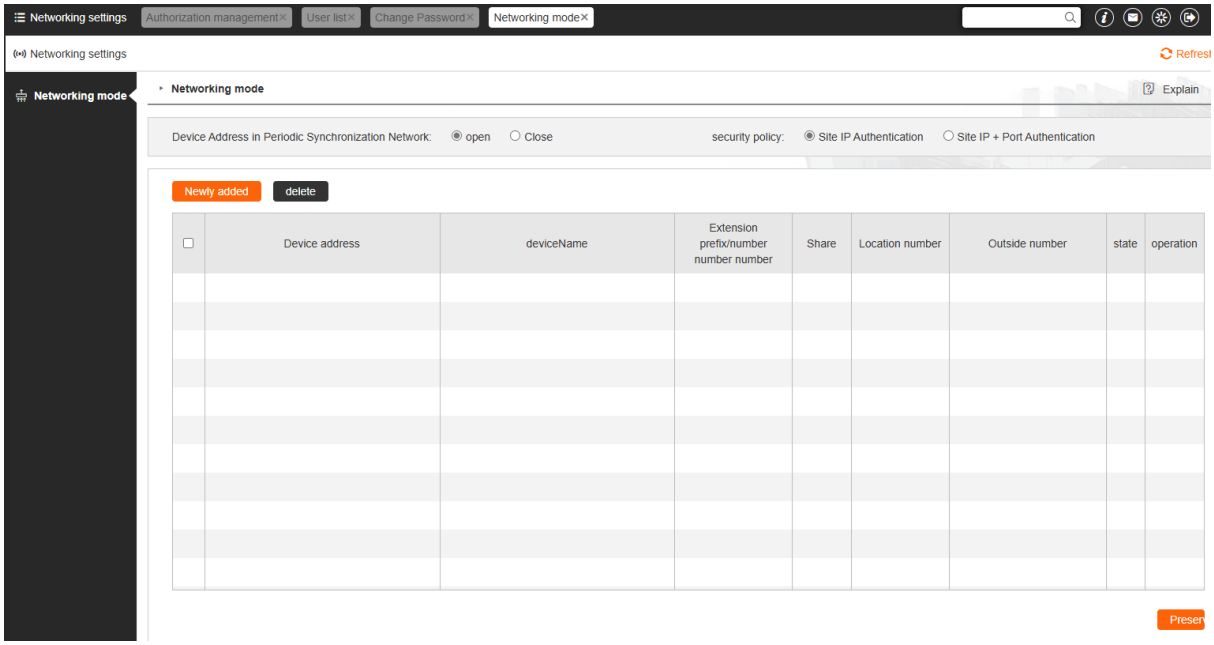


Table3.59 Site Add Interface Parameters

Item	Instructions
device address	Enter the IP addresses and port numbers of the devices participating in the networking. For example, 202.56.209.63:8888. If you do not enter a port number, the default port 5060 is used. The first one is a management site and the others are general sites. Note: If the device is in a private network, you need to do port mapping on the front-end router.
Extension prefix/number digits	Enter a range of extension numbers for the device, e.g., 2/3 means the extension number is a three-digit number beginning with 2. Note: The extension prefixes of the devices in the network cannot conflict. For example, devices A and B with prefixes 2/3 and 21/3, respectively, conflict because if both devices have extension 210, users of device A cannot dial extension 210 of device B. Calls dialed 210 are sent to extension 210 of device A.
enjoy together	• Checked: The device's outside line is allowed to be used by other devices. • Unchecked: The device's outside line is not allowed to be used by other devices.

 Copyright © Redstone Systems, Inc

Item	Instructions
area code	Other device extensions dialing directly to a number beginning with this area code can be called out through this device (this configuration cannot be configured the same on each device). For example, site A fills in the area code 8, allowing its outside line to be shared with other sites in the network. When other sites call the number 61202777 by dialing 861202777, it will be called through site A's outside line, and site A will automatically remove the area code 8 to call 61202777. Note: Avoid zone number configurations that conflict with other site local number resources. For example, the area code "021" will conflict with the default dialing of "0" to call the switchboard at other sites (this conflict only exists when the dialing rule at other sites is to add prefixes to outgoing calls).
external number (e.g. telephone)	When the network is interrupted, the extension of other devices in the network calls the extension of this device, you can call the device through the PSTN call "area code" + the "outside number".

Step5. Add another site

Click Add to add information about all general site equipment on the net.

Step6. Update device address

After saving and rebooting. The management site (the first device in the list) will send the information about the address change of the devices in the network to the other devices.

General Site

Step1. Go to Networking Settings>Networking Methods.

Step2. Enable periodic synchronization of device addresses on the network.

Step3. Select the security policy.

Step4. Adding a management site

Click Addand enter the information for the management site on the first line of the list. Fill in the first line of the configuration consistent with that of the management site.

Step5. Add your own information

Click Addand enter information about this device on the second line of the list. Fill in the configuration consistent with that of the management site.

Step6. Update device address

Aftersavingthe settings, the management site (the first device in the list) will send information about the change of address of the device in the network to that device.

 Copyright © Redstone Systems, Inc

4 Common Problems

4.1 IP Outbound Registration Issues

Phenomenon:When making an outgoing call with an IP outside line, you can hear a dial tone, but the call is never dialed.

Solution:

Table4.1 Solution to SIP Outbound Registration Problems

Possible causes	cure
Registration is not responding.	Contact your IP telephony service provider to confirm that the address of the SIP outbound registration server is correct; test whether the network between the device and the registration platform is normal.
Incorrect IP outbound registration number.	Contact your IP telephony service provider to confirm that the SIP outbound registration number is correct.
Incorrect registration password.	Contact your IP telephony service provider to confirm that the SIP outbound registration password is correct.

 Copyright © RedStone Systems, Inc