

New Rock Technologies, Inc.

OM Series IP Telephony System

OM8000

Administrator's Manual

Document Version: 02

Release Date: 2024-12-16

Amendment Records

Document **Rev. 01**

Full Text.

Copyright © 2025 New Rock Technologies, 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 OM8000.

This guides administrators to parameterize the OM through the web interface. Some of the parameters can also be set via the handset, for details see [OM User's Manual](#).

Web site:<http://www.newrocktech.com>

Documentation Center:<https://www.newrocktech.com.cn/DocumentCenter>

Contents

Amendment Records	2
Manual Description	3
Contents	4
Contents of Figures	7
Contents of Tables	9
1 Overview	11
1.1 Overview	11
1.2 Product Characteristics	12
1.3 Product Specification	13
1.4 Hardware And Software Module Composition	14
2 Configuring Basic Functions	17
2.1 Logging in to the Web	17
2.2 Configuration Wizard	18
2.2.1 Step 1: Hardware Confirmation	18
2.2.2 Step 2: Network Configuration	19
2.2.3 Step 3: IP Extensions	19
2.2.4 Step 4: SIP Outbound	20
2.2.5 Step 5: Outbound Calling Rules	20
2.2.6 Step 6: Configuration Completed	21
3 Configure Personalization Features	22
3.1 Condition Monitoring	22
3.1.1 Device Status	23
3.1.2 Extension Status	26
3.1.3 Outsider Status	27
3.1.4 System Status	29
3.2 Basic Settings	33
3.2.1 Network Setup	33
3.2.2 Outgoing Rule	38
3.2.3 Central Exchange	40
3.2.4 Multi-level IVR	45
3.2.5 Voice management	49
3.3 Extension Setup	52

3.3.1 IP Extension	52
3.3.2 Sectoral	63
3.3.3 Caller ID Binding Form	65
3.4 External line setup	66
3.4.1 SIP Outbound	66
3.4.2 Directly Connected Repeater Group	75
3.4.3 DOD Number	76
3.5 Application Service	77
3.5.1 Media, Esp. News Media	77
3.5.2 API	78
3.5.3 Sound Recordings	82
3.5.4 Call Barring	83
3.5.5 Secretary	84
3.5.6 Duty Roster	85
3.6 Advanced Settings	91
3.6.1 Systems	91
3.6.2 Certificates	93
3.6.3 Function Code	93
3.6.4 Dial Detection and Bitmap	95
3.6.5 SIP Compatibility	97
3.6.6 Routing Table	99
3.6.7 Network Management	107
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	119
3.8.3 Alarm Management	121
3.8.4 Configuration Management	124
3.8.5 Version Management	125
3.8.6 Log Management	125
3.8.7 System Tools	127
3.9 Rights Management	135
3.9.1 User List	135
3.9.2 Operating Log	136
3.9.3 Modify A Password	137

3.10 Network Setup	138
4 Common Problems	142
4.1 IP Outbound Registration Issues	142

Contents of Figures

Figure1-2 Front panel	14
Figure1-3 Rear panel	15
Figure2-1 login screen	17
Figure3-1 switching mode	34
Figure3-2 802.1X Configuration Interface	38
Figure3-3 Auto Attendant Configuration Screen	40
Figure3-4 IVR1 Configuration Interface	48
Figure3-5 Background Music Configuration Interface	51
Figure3-6 Number Filtering Configuration Interface	63
Figure3-7 Department Configuration Screen	64
Figure3-8 Incoming Call Binding Table Screen	65
Figure3-9 SIP Outbound New Interface	66
Figure3-10 SIP Outbound Configuration Interface	69
Figure3-11 SIP Outbound Registration Options Screen	72
Figure3-12 Linear (DID/DOD) Configuration Interface	77
Figure3-13 Media Configuration Interface	77
Figure3-14 API Configuration Interface	79
Figure3-15 Remote Recording Configuration Interface	82
Figure3-16 Extension Recording Configuration Interface	82
Figure3-17 Call barring configuration screen	84
Figure3-18 Attribution area code configuration screen	92
Figure3-19 DTMF interface	92
Figure3-20 Function Code Configuration Screen	94
Figure3-21 Dialing Rule Configuration Screen	95
Figure3-22 SIP Compatibility Interface	97
Figure3-23 Routing Table Configuration Interface	99
Figure3-24 Routing Table Configuration Interface - Call Length Restriction	102
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	138
Figure3-40 Network Configuration Interface	139
Figure3-41 Add Site Screen	139

Contents of Tables

Table1-1 Performance specifications	13
Table1-2 Hardware Specifications	13
Table1-1 Indicator light meaning table	15
Table1-2 Interface Description	16
Table2.1 Login Interface Parameters	18
Table3-1 Description of Device Status	25
Table3-2 Description of Equipment Name	33
Table3-3 Parameter description	34
Table3-4 IMS Dedicated Access Mode Parameter Description	36
Table3-5 802.1X Interface Parameter Description	38
Table3-6 Outbound call rule parameter description	39
Table3-7 Automated Operator Parameters	41
Table3-8 Factory Default Voice File	41
Table3-9 Microphone Recording Welcome Note	42
Table3-10 Operator Configuration Screen	44
Table3-11 Operator Parameters	44
Table3-12 Multi-level IVR	47
Table3-13 Multi-level IVR	48
Table3-14 IP Extension Configuration Parameter Description	53
Table3-15 IP Extension Configuration Parameter Description	59
Table3-16 IP Extension Parameter Description	62
Table3-17 Parameter Description of Number Filtering Interface	63
Table3-18 Parameter Description of Sectoral	64
Table3-19 Parameter Description of Caller Binding Number Form	65
Table3-20 Description of SIP outbound registration parameters	67
Table3-21 SIP Outbound Interface Parameter Description	69
Table3-22 Parameter Description of SIP Outbound Registration Options	72
Table3-23 Description of media parameters	78
Table3-24 API Interface Parameter Description	79
Table3-25 Extension API Switch Parameter Description	80
Table3-26 Outside API switch Parameter Description	81
Table3-27 Outside API switch Parameter Description	85
Table3-28 Duty roster Parameter Description	87
Table3-29 Duty roster Parameter Description	88

Table3-30 Duty roster Examples	89
Table3-31 Explanation of attributed area code parameters	92
Table3-32 DTMF Parameter Description	93
Table3-33 Function code Parameter Description	94
Table3-34 Explanation of the rules of the common numbered digit map	96
Table3-35 SIP Compatibility Parameter Description	97
Table3-36 Interface Configuration Rules Description	100
Table3-37 Interface Configuration Rules	103
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	122
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	134
Table3-58 Security Policy Parameters	139
Table3-59 Site Add Interface Parameters	140
Table4-1 Solution to SIP Outbound Registration Problems	142

2 Overview

2.1 Overview

OM8000 converged communication platform is a new generation of IP voice core switching equipment launched by New Rock, to meet 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, to provide voice calls, video calls, high-speed faxes, teleconferencing, telephone recording, mobile extensions, and other integrated converged communication solutions.

OM8000 has powerful call processing capability, supporting 8000 user access and 800 simultaneous calls. It also excels in stability, reliability, security, scalability and configuration flexibility.

OM8000 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, and also 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.

2.2 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, liquor 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-machine hot standby, master and standby 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

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

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

Use in conjunction with the Xun Shi equipment unified management system

2.3 Product Specification

Table1-1 Performance specifications

Item	Description
IP extension license	kind
IP Outside License	8,000 road
Number of simultaneous calls	800-way (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 stacking: 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	Single card supports 1000 IP extensions, 125 concurrent calls (with

Item	Description
Resource Card	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 Configuration Interface	RJ45
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°C ~ 40°C; Relative humidity: 10% ~ 90% (non-condensing)
Storage Environment	Temperature: -40°C ~ 70°C; Relative humidity: 5% ~ 90% (non-condensing)
Height Above Sea Level	Below 2000 meters
Climatic Conditions	Recommended non-tropical

2.4 Hardware And Software Module Composition

Figure2-2 Front panel

Single machine



Dual-player



Figure2-3 Rear panel

Single machine



Dual-player



Table1-1 Indicator light meaning table

Indicator light	Flashing status	Particular
Pwr (Green)	Green and bright	Power on.
	Go out (of fire)	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
	Go out (of fire)	deactivate
Run	Green and bright	The power supply is normal.
Alm (Red, Green)	Go out (of fire)	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)

Indicator light	Flashing light status	Particular
Mesh Port Lights (Left And Right Sides)	Long green light on the right side	1000Mbps
	Right side off	10/100Mbps
	Long green light on the left side	Physical link established, but no business flow
	Shiny green on The left side	Physical links have been established and there is a business Flow
	Left side off	No physical link established

Table1-2 Interface Description

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

3 Configuring Basic Functions

3.1 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.

Figure3-1 login screen



Table2.1 Login Interface Parameters

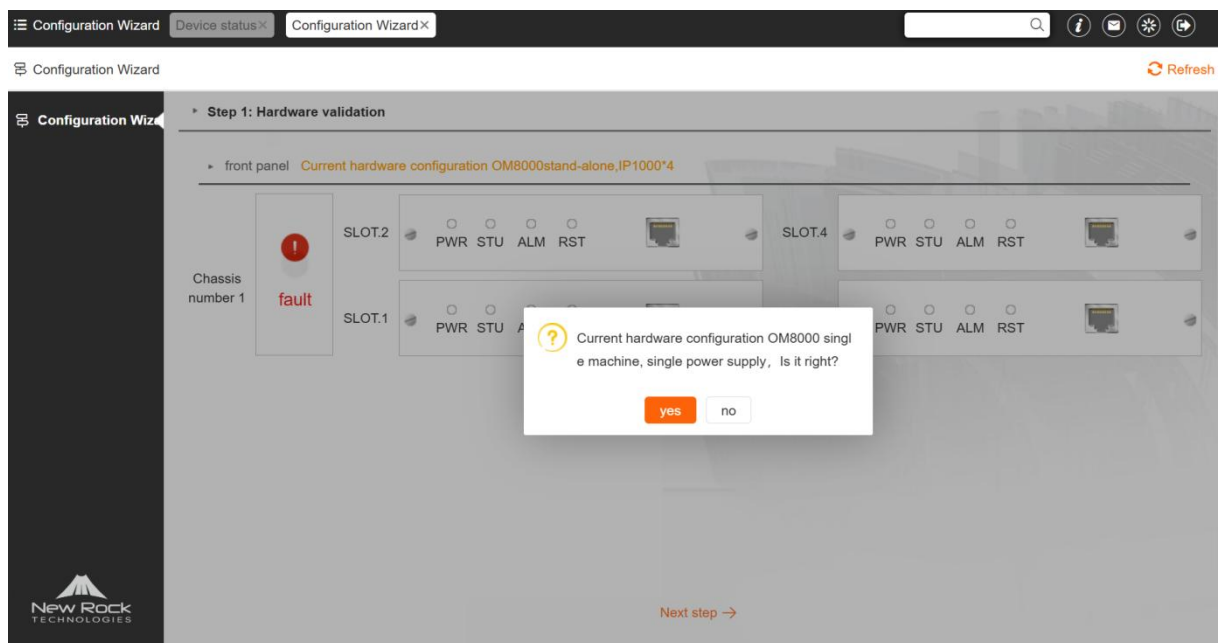
Item	Description
Medium EN	Select the interface language as Chinese or English.
Dignity	The device provides two levels of administrative privileges: ● admin: the default super administrator of the system. ● Ordinary Administrator: account is created by admin after logging in to the device, and account permissions are defined by admin when it is created. The system can have multiple general administrator accounts.
Cryptographic	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.

3.2 Configuration Wizard

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

3.2.1 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.



3.2.2 Step 2: Network Configuration

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

Stand-alone

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

► Step 2: Network Configuration

1Number machine

IP address:	192 . 168 . 191 . 128	Subnet mask:	255 . 255 . 254 . 0	default gateway:	192 . 168 . 190 . 1
Main DNS:	114 . 114 . 114 . 114	Prepare DNS:	. . .		

Dual-player

In the dual 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.

3.2.3 Step 3: IP Extensions

Configuration Wizard | Device status | Configuration Wizard

Configuration Wizard

► Step 3: IP Extension

*Initial extension number:

DOD Generation Mode: Use the same number ▼

Initial Trombone:

*Lot size: Add up to 1000 at a time.It can be used:5990

Registration Password Generation: empty ▼

IP Address When Using IP Authentication:

Expiration authority: Inside line ▼

CRBT: Please choose ▼

open: ☒ Caller ID ☐ Sound recording

Call transfer: Please choose ▼

Monitor: Please choose ▼

← Previous step ⚡ skip Next step →

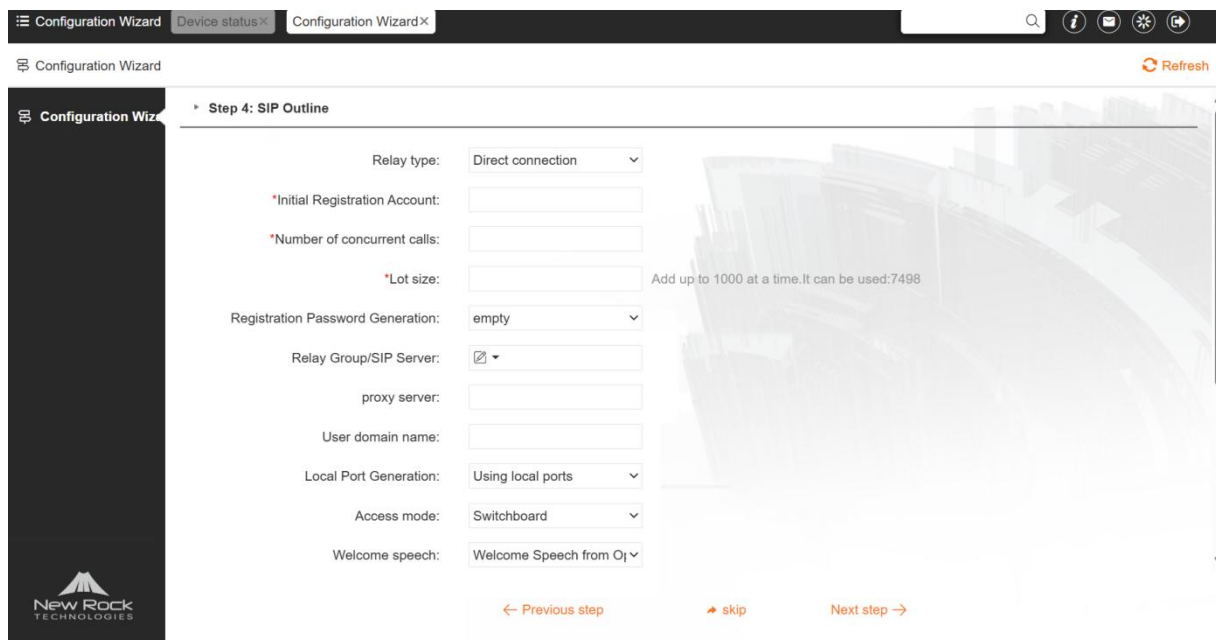
New Rock TECHNOLOGIES

For a description of the parameters, seeTable3.14 *This step can be skipped

3.2.4 Step 4: SIP Outbound

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

*This step can be skipped

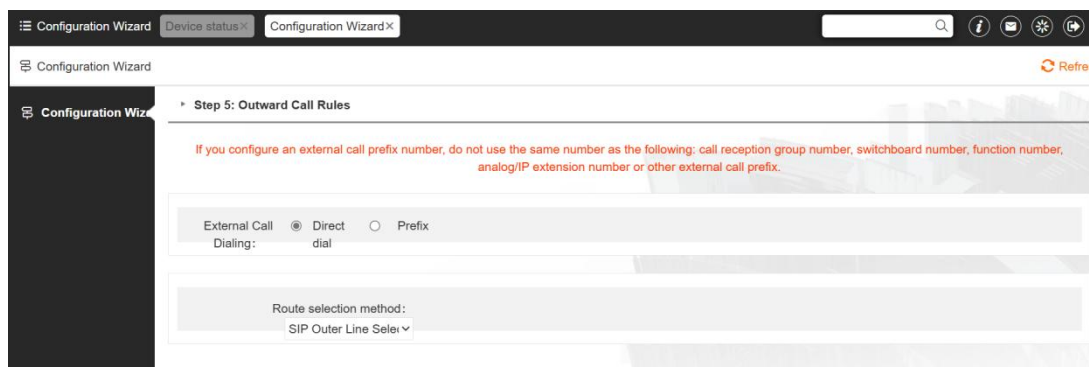


The screenshot shows the 'Step 4: SIP Outline' configuration screen. The interface includes a sidebar with 'Configuration Wizard' and 'Device status' tabs. The main area contains the following fields:

- Relay type: Direct connection (dropdown)
- *Initial Registration Account: (text input)
- *Number of concurrent calls: (text input)
- *Lot size: (text input) with a note: 'Add up to 1000 at a time. It can be used: 7498'
- Registration Password Generation: empty (dropdown)
- Relay Group/SIP Server: (text input with a plus icon)
- proxy server: (text input)
- User domain name: (text input)
- Local Port Generation: Using local ports (dropdown)
- Access mode: Switchboard (dropdown)
- Welcome speech: Welcome Speech from Oj (dropdown)

At the bottom, there are navigation buttons: 'Previous step' (left arrow), 'skip' (flame icon), and 'Next step' (right arrow). A 'Refresh' button is in the top right corner.

3.2.5 Step 5: Outbound Calling Rules



The screenshot shows the 'Step 5: Outward Call Rules' configuration screen. The interface includes a sidebar with 'Configuration Wizard' and 'Device status' tabs. The main area contains the following fields:

- A warning message: 'If you configure an external call prefix number, do not use the same number as the following: call reception group number, switchboard number, function number, analog/IP extension number or other external call prefix.'
- External Call Dialing: Direct (selected radio button) or Prefix (radio button)
- Route selection method: SIP Outer Line Sele (dropdown)

A 'Refresh' button is in the top right corner.

*This step can be skipped

2.2.6 Step 6: Configuration Completed

► Step 6: Configuration complete

Hardware			
Current hardware configuration	OM8000 single machine, IP1000 * 4, single power supply		

Network			
Chassis 1	IP address:	Subnet mask:	default gateway: 192.168.190.1
	192.168.191.128	255.255.254.0	
	Main DNS:	Prepare DNS:	
	114.114.114.114		

[← Previous step](#)

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

4 Configure Personalization Features

4.1 Condition Monitoring

Status monitoring provides query on equipment status, extension status, outside line 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.

Outside line status: presents the usage of the device's outside lines, including the overall status as well as the status of each line.

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

4.1.1 Device Status

Go to **Status Monitor>Device StatusView**.

Front Panel

Displays the fan/daughter card status of the corresponding chassis.

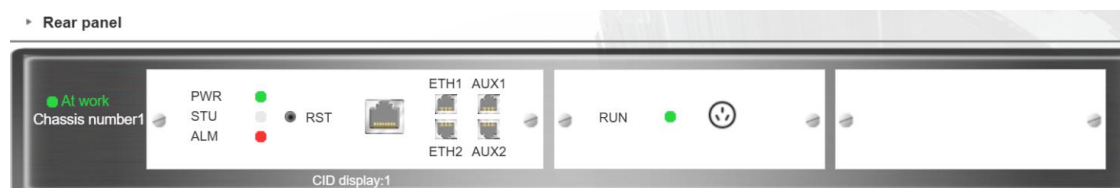


Click on a subcard to display the version information for that subcard.



Rear Panel

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



Subscriber Call

Displays extension and outside line online status, call status, etc.

 User talk	
IP Extension Online	1000
IP External Online	0
IP Extension is on the phone	0
IP Outline is on the phone	0
Running time	0day0hour14min
Recent startup time	2024-12-17 16:23:22

Alarm Center

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

 Alarm Center	
urgent	7
important	0
commonly	1
Jump to the alarm center	

Security Center

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

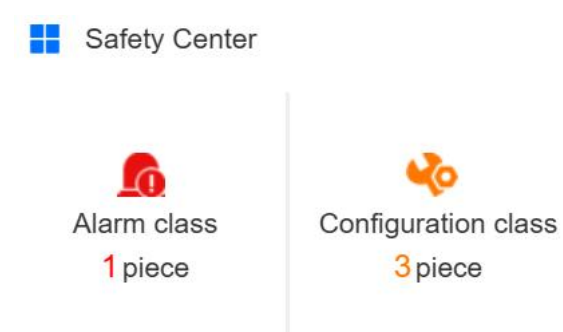


Table3-1 Description of Device Status

Item	Description
Warning Category	be 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.

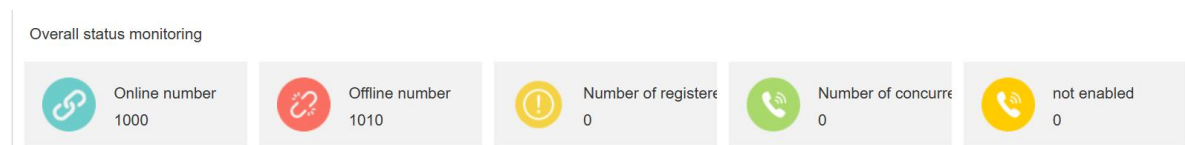
Item	Description
	There is no long distance call duration limitation, please go to "Long Distance Call Limitation" to configure.
	Default administrator password has not been changed

4.1.2 Extension Status

Go to **Status Monitor>Extension StatusView**.

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:

Paragraph number:

-

Online state:

Please choose

Extension number	Full name	department	Online state	Last registration time	Registration Terminal IP Address	Registration Terminal IP Address (Hello)	UA	Call state	The other party number	Last call status
60001			Off-line					free		0
60002			Off-line					free		0
60003			Off-line					free		0
60004			Off-line					free		0
60005			Off-line					free		0
60006			Off-line					free		0
60007			Off-line					free		0
60008			Off-line					free		0
60009			Off-line					free		0

Previous page

1

2

3

...

39

40

41

next page

Display per page

- Extension number: Enter the extension number and click "Query" to filter out the extension information.
- Number segment: 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 status, display name, UA, and last registration time.

More screening

department:

Please choose ▾

Call state:

Please choose ▾

Display name:

UA:

Last registration time:

 --

data format:1970-01-01 08:00:00

Determine

cancel

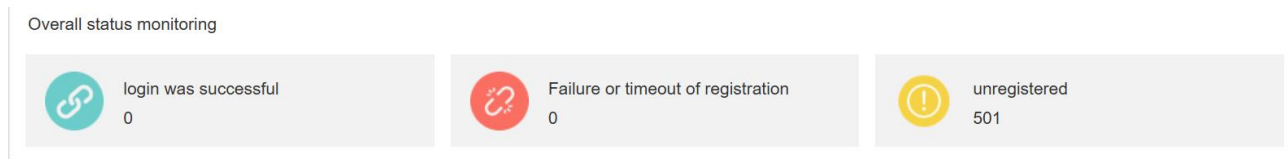
4.1.3 Outsider Status

Go to **Status Monitor>Outside Line StatusView**.

Overall Status Monitoring

Statistics on the number of successful, failed, unregistered, and in-call registrations for

external lines.



Detailed Data

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

Detailed data

Extension number: Paragraph number: - Online state:

Extension number	Full name	department	Online state	Last registration time	Registration Terminal IP Address	Registration Terminal IP Address (Hello)	Registration Terminal IP Address (Hello)	Last call status
60001			Off-line					0
60002			Off-line				free	0
60003			Off-line				free	0

Please choose

- On-line
- login was successful
- IP Address Authentication
- Off-line
- login has failed
- unregistered
- Cancellation

- Outside line number: Enter the outside line number and click "Query" to filter out the information of the outside line.
- Number segment: 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.

More screening

Registration status

Please choose

▼

s:

Outside line type:

Please choose

▼

SIP server address

s:

Determine

cancel

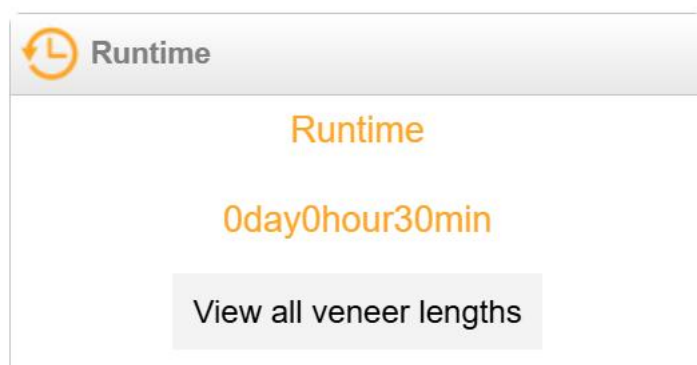
4.1.4 System Status

Go to **Status Monitor>System StatusView**.

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

runtime

Displays the master board runtime. Click "View All Board Hours" to display all board hours.



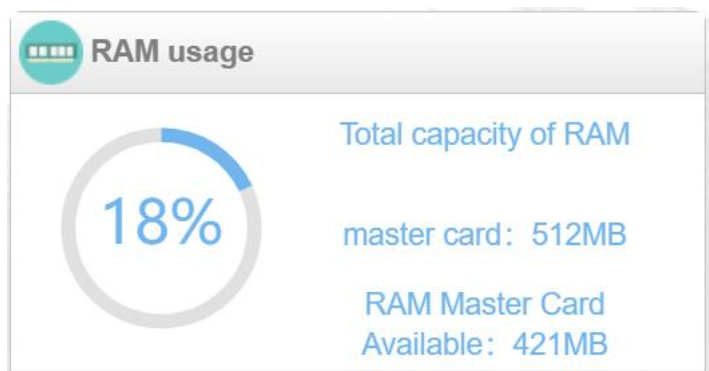
CPU Usage

Displays the CPU occupancy rate. Click "View All Single Board CPU" to display the CPU utilization of all boards.



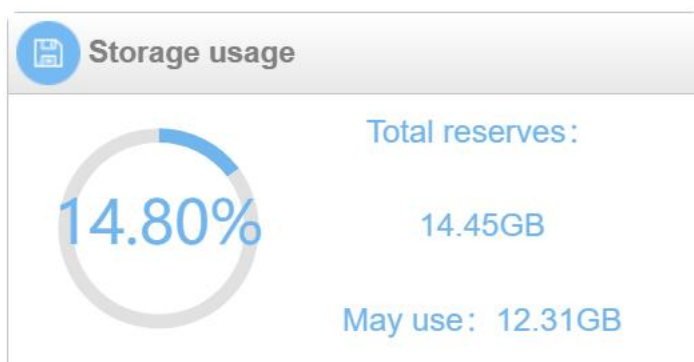
RAM Utilization

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



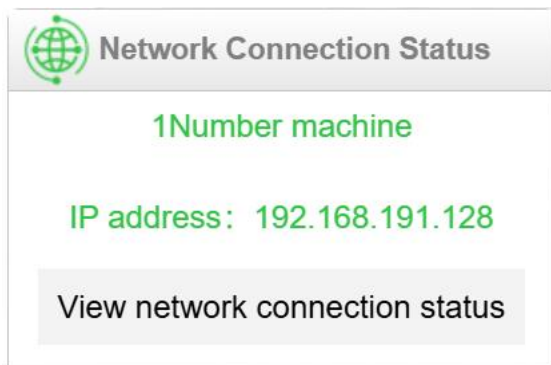
Storage Utilization

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



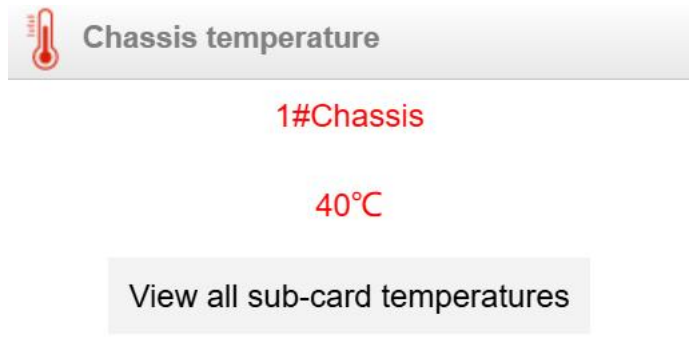
Network Connection Status

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



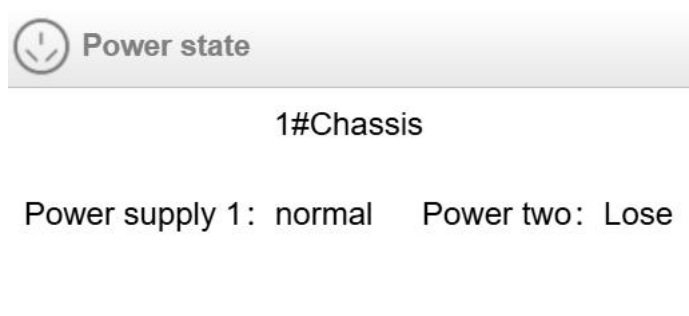
Chassis Temperature

Displays the chassis temperature. Click "View All Daughter Card Temperatures" to display the temperature of each daughter card.



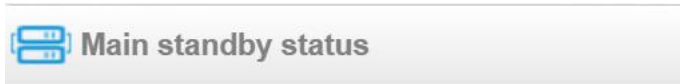
Power State

Displays the power supply operating status.



Master/Backup Status

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



Main standby status

Host (1#) : At work

Standby machine (2#) : Not inserted

Enabled Service Listening Ports



Enabled Service Listener Port

service: No Startup Service

Agreement:

Port number:

Fan (loanword)

Displays the fan status.



Fan

Fan: fault

speed: 0

4.2 Basic Settings

4.2.1 Network Setup

Equipment Name

Go to **Basic Settings>Network Configuration** and configure the device name.

Table3-2 Description of Equipment Name

Item	Description
Equipment 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 OM8000, AUX1 and AUX2, are only used for interconnection between dual machines when double-clicking stacking.

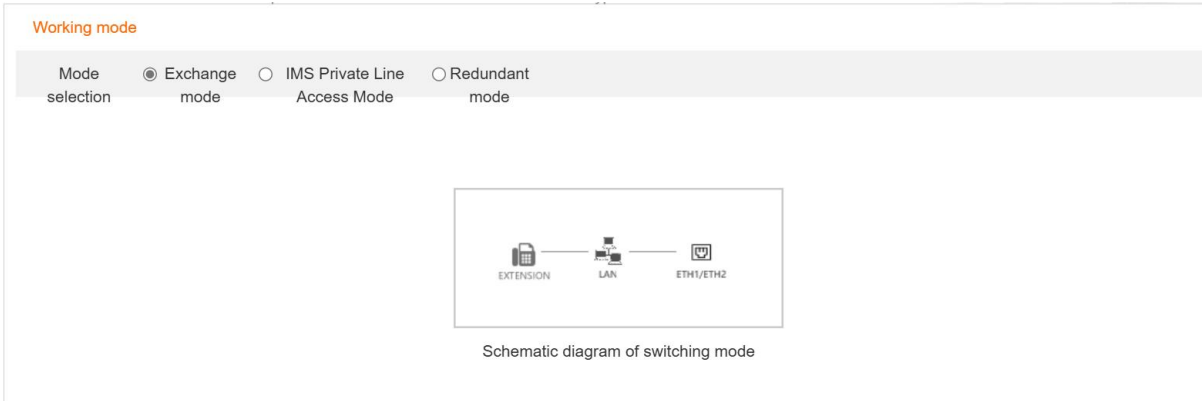
Go to **Basic Settings>Network Configuration** to configure it.

- **Switching Mode**

The ETH1 and ETH2 interfaces are switched to each other and share IP addresses.

Figure4-1 switching mode

Stand-alone



Dual-Player

network configuration

IP address:	192 . 168 . 191 . 128	Subnet mask:	255 . 255 . 254 . 0	default gateway:	192 . 168 . 190 . 1
Main DNS:	114 . 114 . 114 . 114	Prepare DNS:	. . .		

Table3-3 Parameter description

Item	Description
Stand-Alone	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-Player	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: After configuring the subnet mask of the whole machine, the subnet mask of chassis 1 and 2 is the same as that of the whole machine. Gateway address: after configuring the gateway of the whole machine, the gateway of chassis 1 and 2 is the same as that of 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.

● IMS Dedicated 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.

Stand-Alone

Basic setup Refresh

network configuration

Switchboard

Caller Answering Group

Outgoing rule

Voice management

Multilevel IVR

New Rock Technologies

Working mode

Mode selection: ☐ Exchange mode ☒ IMS Private Line Access Mode ☐ Redundant mode



Schema of Access Mode for IMS Private Line

ETH1

IP address: 192 . 168 . 191 . 128 Subnet mask: 255 . 255 . 254 . 0 default gateway: 192 . 168 . 190 . 1

Main DNS: 114 . 114 . 114 . 114 Prepare DNS: . . .

ETH2

Connection mode: Fixed IP address

Dual-Player

ETH1

IP address: 192 . 168 . 191 . 128 Subnet mask: 255 . 255 . 254 . 0 default gateway: 192 . 168 . 190 . 1

Main DNS: 114 . 114 . 114 . 114 Prepare DNS: . . .

ETH2

Connection mode: Fixed IP address

IP address: . . . Subnet mask: . . . default gateway: . . .

Main DNS: . . . Prepare DNS: . . .

Adding other applications: ☐ Application of ☐ PRRecording Server ☐ custom

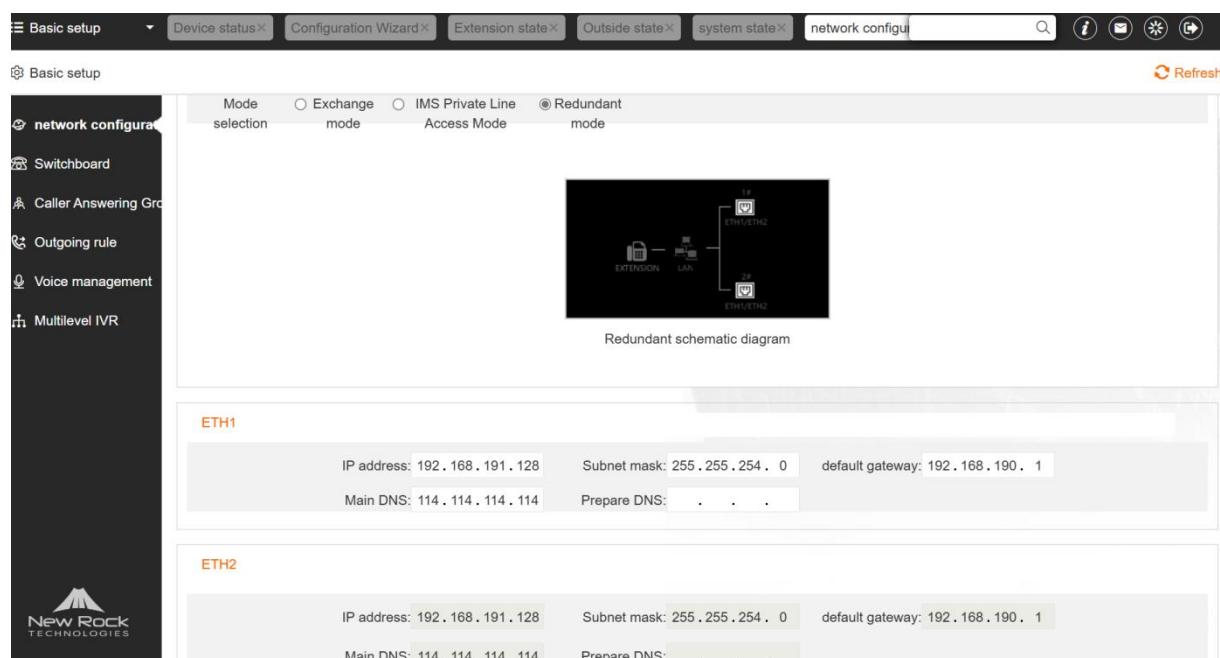
Table3-4 IMS Dedicated Access Mode Parameter Description

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.
Primary DNS	Enter the IP address of the preferred DNS server.
Alternate 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.
Primary DNS	Enter the IP address of the preferred DNS server.
Alternate 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.

● Redundancy Mode

This mode is only applicable in the stand-alone 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.



802.1X

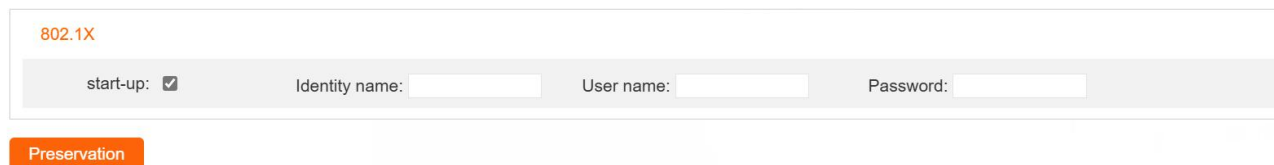
802.1X is an IEEE standard for authentication of users accessing a network, known as Port-Based Network Access Control (PNAC). 802.1X authentication involves three components: the applicant, the authenticator, and the authentication server. The applicant is a client device that needs to connect to a 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 OM supports 802.X and acts as an applicant, requiring 802.X to be enabled on the OM when the network requires 802.1X authentication.

Go to **Basic Settings>Network Configuration** to enable 802.1X.

Figure4-2 802.1X Configuration Interface



The screenshot shows the 802.1X configuration interface. At the top, there is a section titled "802.1X" in orange. Below it, there is a "start-up:" checkbox which is checked. To the right of the checkbox are three input fields: "Identity name:", "User name:", and "Password:". Below these fields is an orange button labeled "Preservation".

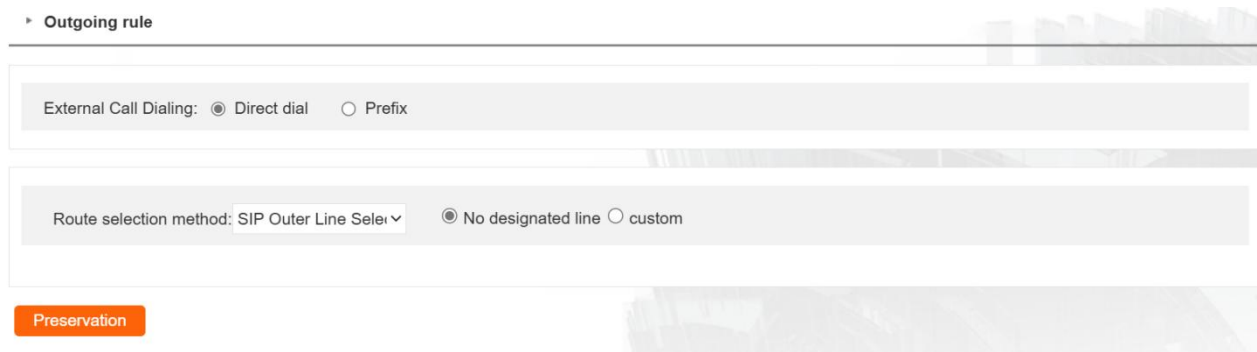
Table3-5 802.1X Interface Parameter Description

Item	Description
Activate (A Plan)	Enable the 802.1X function.
Identity Name	Identity for authentication, provided by the authentication server
User ID	Username for authentication, provided by the authentication server
Cryptographic	Password for authentication, provided by the authentication server

4.2.2 Outgoing Rule

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

Dial Direct



The screenshot shows the "Outgoing rule" configuration interface. At the top, there is a section titled "Outgoing rule" with a right-pointing arrow. Below it, there is a section titled "External Call Dialing:" with two radio buttons: "Direct dial" (which is selected) and "Prefix". Below this section is another section titled "Route selection method:" with a dropdown menu showing "SIP Outer Line Seler" and two radio buttons: "No designated line" (which is selected) and "custom". Below these sections is an orange button labeled "Preservation".

Prefix

Click **Add** to add a prefix.

Table3-6 Outbound call rule parameter description

Item	Description
Outbound Dialing Method	Direct dialing:Extension users dial internal extension numbers and external numbers directly. Add Prefix:Extension users dial internal extension number directly and 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 Shun 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, and 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 (Linguistics)	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 outgoing line down-select, the device selects the SIP outgoing line to call the other party according to the down-select method when the user dials 9 before dialing the outgoing line. Note 1: This parameter is configurable only when the Outbound Dialing Method is Add Prefix. Note 2: The Outgoing Call Pickup Line Prefix cannot conflict with extension numbers, group numbers of Call Pickup Groups, feature codes and other Outgoing Call Pickup Line Prefix numbers.
Second Dial Tone	After the extension user dials the outgoing call selector prefix, the device provides a secondary 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 (E.G. Railway)	Specify the prefix corresponding to the outgoing line number, i.e., the number of each outgoing line corresponding to the selection of SIP outgoing lines for downstream and round selection. You can select the outside number directly or enter it manually, with half 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.

4.2.3 Central Exchange

Automated Operator

The Auto Attendant feature is where the OM plays voice navigation (welcome message) to the caller after connecting an outgoing call. Voice navigation in OM 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.

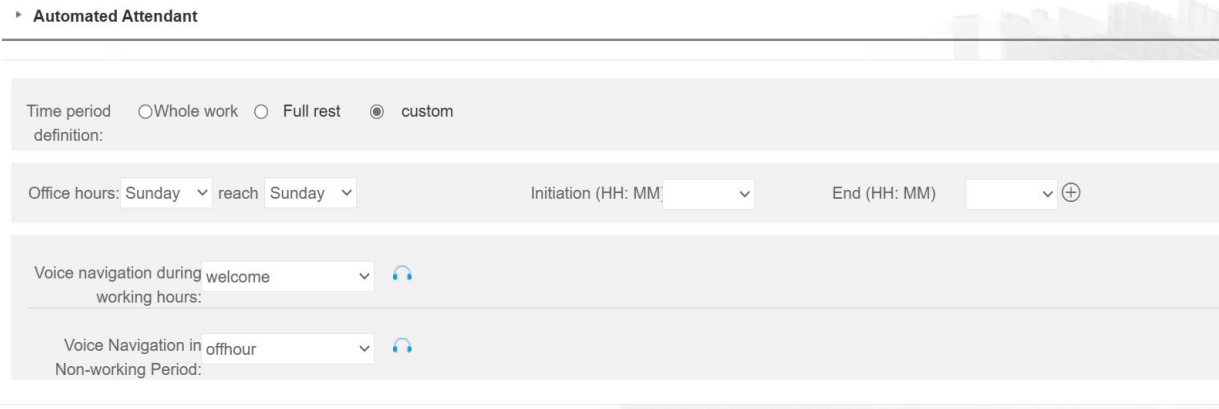
Follow the steps below to configure the voice navigation used by the automated attendant:

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

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

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

Figure4-3 Auto Attendant Configuration Screen



Automated Attendant

Time period ☐ Whole work ☐ Full rest ☒ custom

definition:

Office hours: Sunday reach Sunday Initiation (HH: MM) End (HH: MM) ⊕

Voice navigation during welcome working hours: 

Voice Navigation in offhour Non-working Period: 

Table3-7 Automated Operator Parameters

Item	Description
Definition Of Time Slots	Full work:always play the work hour welcome message. Full break:always play the welcome message during non-working hours. Customize: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, outgoing calls during the time slot are heard as work-slot voice navigation, and times outside the time slot are heard as non-work-slot 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, if you need to change it, you need to prepare the voice file first, see Customizing and replacing voice files . If you want to change the voice file, you need to prepare the voice file first, see - To set up a multi-level IVR, click Add IVR. For specific production see 3.2.4 . Click Auditionto 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 working hours, if you want to change it, you need to prepare the voice file first, see Customizing and replacing voice files . If you want to change the voice file, you need to prepare the voice file first, see - To set up a multi-level IVR, click Add 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	Welcome to your call, please dial the extension number directly, and dial 0 for number checking.
Non-Working Hours	offhour	We welcome your call. It's after hours, so please dial the extension number directly.

You can also prepare voice files as follows.

- Upload an existing welcome message
- Microphone recording welcome message

1) Upload Welcome Message

Step1. Click **Basic Settings>Voice Management>Upload Welcome Message**.

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

► Voice management

Wind Sound Software CRBT upload Welcome Speech

upload

1.File name: can be composed of letters, numbers and underscores "" and must start with "user", up to 19 characters.
2.File properties: must be 8.000 kHz, 16 bits or 22.050 kHz, 16 bits of mono. wav file, and file size should not exceed 1.5 MB.

Name	type	Background music	operation
user_welcome2205ZH	Welcome speech	☐	

2) Microphone Recording Welcome Message

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	Take off the phone and dial *81, start recording after the voice prompt, and hang up directly after recording.
Give Sb An Audition	Take off the phone and dial *8200 to listen to the temporarily stored voice file.
Save (A File Etc) (Computing)	• Take off the phone and dial *8301 and then hang up to replace the work slot welcome message WELCOME; • Offhook dial *8302 and then hang up to replace the offhour welcome message offhour.
Hearing Of Welcome	• Take off the phone and dial *8201 to hear the saved work slot welcome

Item	Description
Messages Currently In Use	message; Take the machine off the hook and dial *8202 to hear a saved welcome message for non-working hours.
Resumption	Take off the phone and dial *8300 to restore the replacement of the previous voice file.



注意

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 Settings>Switchboard** to configure items related to the **Operator group**.

Table3-10 Operator Configuration Screen

The screenshot displays the 'Operator Configuration' screen. On the left is a sidebar with navigation options: Basic setup, network configuration, Switchboard, Caller Answering Group, Outgoing rule, Voice management, and Multilevel IVR. The main area is titled 'Basic setup' and includes a 'Refresh' button. It contains several sections: 'Time period definition' with radio buttons for 'Whole work', 'Full rest', and 'custom'; 'Voice navigation during welcome working hours' and 'Voice Navigation in offhour Non-working Period' with dropdown menus and speaker icons; an 'Operator' section with a warning message and a 'group' section with a 'Switchboard' input field and a 'traffic distribution' section with radio buttons for 'Sequential selection' and 'Wheel'; a 'Transfer operator, please dial' input field; and an 'Inbound Non-dial Overtime Processing' section with a dropdown menu and a 'Second switchboard' input field. At the bottom, there is a 'Preservation' button.

Table3-11 Operator Parameters

Item	Instructions
Central Exchange	Fill in the extension number of the extension acting as an operator. Up to 5 can be set, with English commas separating the numbers. Extensions filled in here automatically disable Call Waiting, Do Not Disturb, and Call Forwarding.
Voice Allocation	When there is more than one operator extension, you can select the call distribution method. ● Down 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 the phone talks. 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".
To Switchboard, 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.
Number Of Rings	When an outside caller dials an extension and the number of times the

Item	Instructions
Before Turning To Voice Prompts	extension rings reaches the set value (the default number is 10), the device plays a voice prompt to the caller.
Inbound Non-Dialing Timeout Handling	When an outside 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.

4.2.4 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. The second level of the corresponding two menus allow the user to further select "product ordering" and "technical consulting" under the sub-business. In addition to this, the user can choose to return to a higher level 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 Settings>Multilevel IVR**.

Step2. Click **Add** 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**.

▸ Multilevel IVR

Newly added

Name	describe	series	operation

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

▸ Multilevel IVR

234



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

Add IVR

New IVR

Select an existing IVR

Name: 234-1

Prompting language: nothing ▾

Number of Tips Played: 1 ▾

Direct dial extension allowe ☐

describe:

Language types: default ▾

Waiting for button timeout: (Range: 0-300)

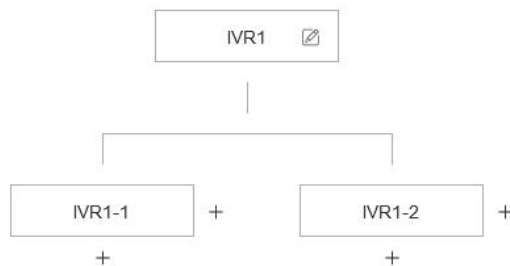
Determine

Return

Table3-12 Multi-level IVR

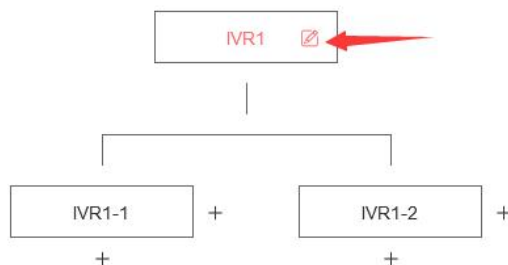
Item	instructions
Item	Consists of letters, numbers, hyphens and underscores, and is no more than 20 characters long.
Descriptive	Describe the use of voice navigation at this level.
Clue	Select a voice file for broadcasting. Voice files need to be prepared in advance.
Language Type	For multilingual IVR. 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 Times The Cue Is Played	The number of times a voice file is played without the caller dialing. The default is 1 time.
Direct-Dial Extensions Are Permitted	When checked, dialing an extension number is allowed during voice file playback.
Waiting For Keystroke 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.

Figure4-4 IVR1 Configuration Interface

▸ 多级IVR

IVR

Name: 234

describe: 4422

Prompting language: user_welcome2205ZH

Language types: default

Number of Tips Played: 1

Waiting for button timeout: 0 second(Range: 0-3)

Direct dial extension allowed: ☐

Key 提示: 按键与号码或前缀不可冲突

Key1: --

Key2: --

Key3: --

Key4: --

Key5: --

Key6: --

Key7: --

Key8: --

Key9: --

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 theBasic Settings > Switchboardpage. ● 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. You need to configure the extension group (call answering group) in theBasic Settings>Call Answering Groupspage beforehand. ● Go 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.

4.2.5 Voice management

Wind Sound Software Upload

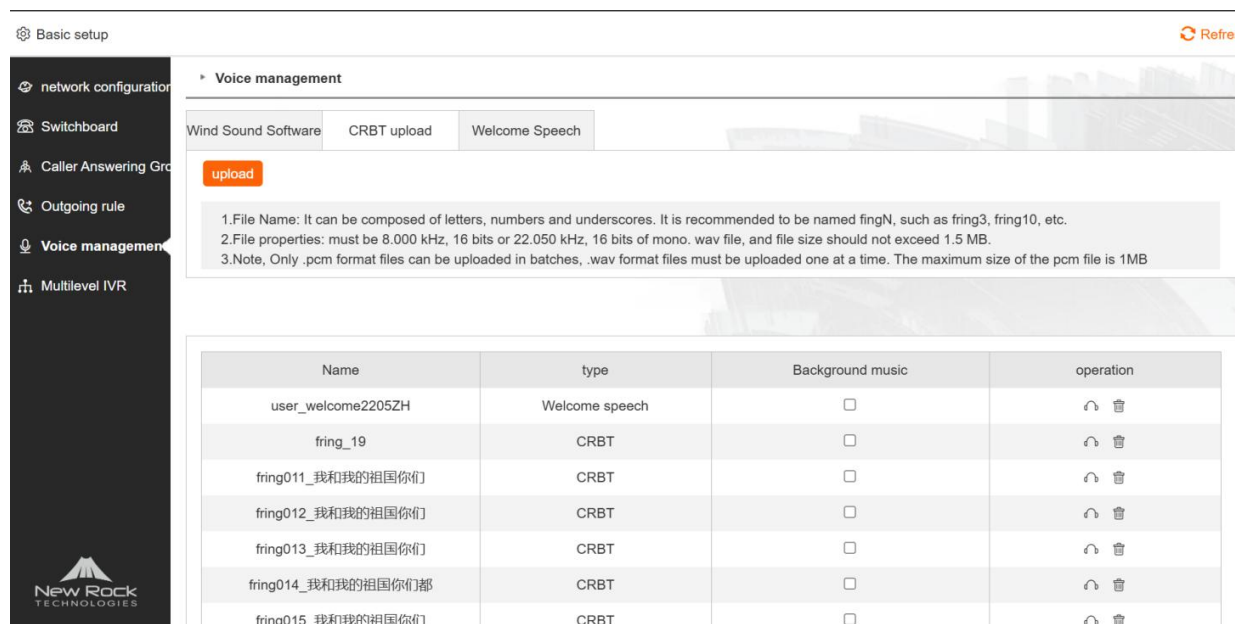
We recommend downloading and installing the "Wind Sound" software. When the format of the voice files for ringtones and welcome messages does not meet the requirements, you can use the "Wind Sound" software to convert the format, and then upload the voice files in the "Ringtone Upload" and "Welcome Message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

Click **BasicSettings>VoiceManagement>Wind Sound Software Upload**, click **Download**, and install the software manually after the download is complete.

The screenshot shows the 'Voice management' section of the configuration tool. On the left is a sidebar with navigation options: Basic setup, network configuration, Switchboard, Caller Answering Group, Outgoing rule, Voice management (selected), and Multilevel IVR. The main area has tabs for 'Wind Sound Software', 'CRBT upload', and 'Welcome Speech'. A message box states: 'Installation of "Wind Sound" software can simplify the process of welcoming words/color bells upload, and provide you with a higher quality voice conversion function. immediatelydownloadAnd install "Wind Sound" after installation, please press F5 to refresh'. Below this is a table with columns: Name, type, Background music, and operation.

Name	type	Background music	operation
user_welcome2205ZH	Welcome speech	☐	
fring_19	CRBT	☐	
fring011_我和我的祖国你们	CRBT	☐	
fring012_我和我的祖国你们	CRBT	☐	
fring013_我和我的祖国你们	CRBT	☐	
fring014_我和我的祖国你们都	CRBT	☐	
fring015_我和我的祖国你们	CRBT	☐	

Ringtone Upload



Step1. Click **Basic Settings>Voice Management>Color Ringtone 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

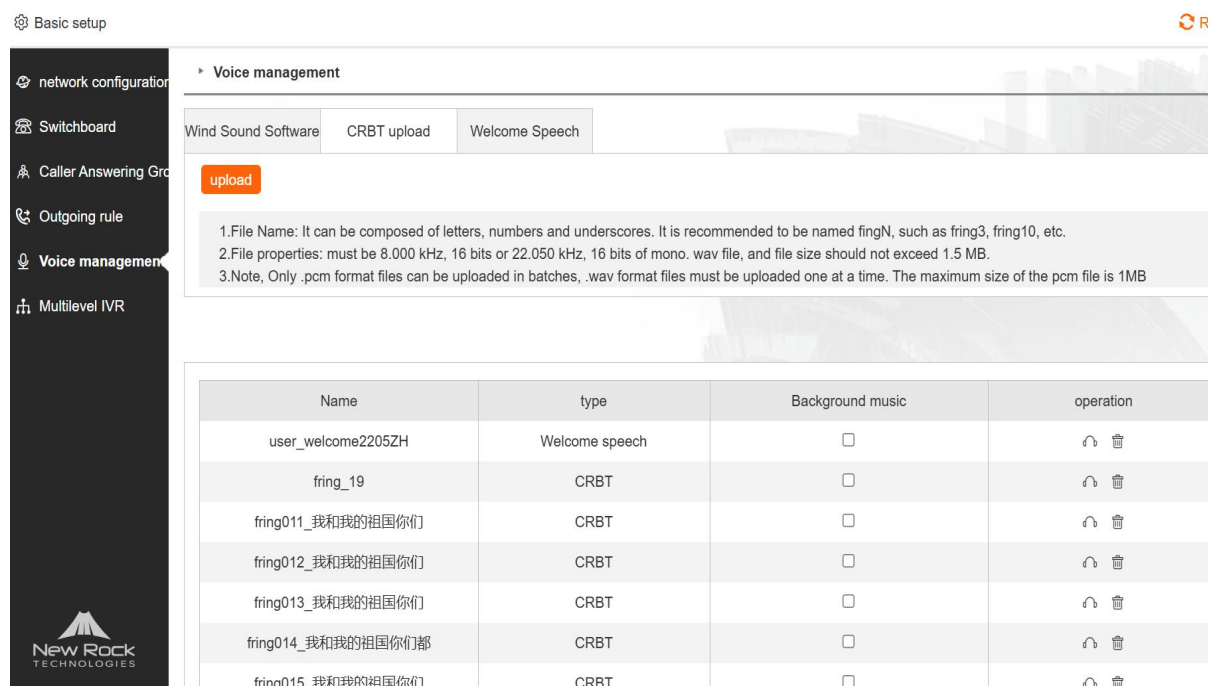
as follows:

Step1. Go to **BasicSettings>VoiceManagement>Color Ringtone 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.

Figure4-5 Background Music Configuration Interface



Welcome Message Uploaded

Click **Basic Settings>Voice Management>Upload Welcome Message**.

The uploaded file must fulfill the requirements in the page.

Basic setup

network configuration

Switchboard

Caller Answering Group

Outgoing rule

Voice management

Multilevel IVR

Wind Sound Software CRBT upload Welcome Speech

upload

1.File name: can be composed of letters, numbers and underscores "" and must start with "user", up to 19 characters.
2.File properties: must be 8.000 kHz, 16 bits or 22.050 kHz, 16 bits of mono. wav file, and file size should not exceed 1.5 MB.

Name	type	Background music	operation
user_welcome2205ZH	Welcome speech	☐	
fring_19	CRBT	☐	
fring011_我和我的祖国你们	CRBT	☐	
fring012_我和我的祖国你们	CRBT	☐	
fring013_我和我的祖国你们	CRBT	☐	
fring014_我和我的祖国你们都	CRBT	☐	

New Rock TECHNOLOGIES

4.3 Extension Setup

4.3.1 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 OM.

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

Extension settings

IP extension

Extension number: Paragraph number: Online state: whole

No screening conditions

Newly added Generating NRP Phone Profile delete (Delete all if no item selected)

Number of Extensions Available: 5990 Number of Extensions Used: 2010

	line	Extension number	Online state	Enable	DOD number	Registration password	Authorization Code (PIN Code)	department	Display name	Expiration authority	CPN	Invitation code	operation
☐	1	60001	Off-line	☒		*****				internation	680114	See	
☐	2	60002	Off-line	☒		*****				internation	680114	See	
☐	3	60003	Off-line	☒		*****				internation	680114	See	
☐	4	60004	Off-line	☒		*****				internation	680114	See	
☐	5	60005	Off-line	☒		*****				internation	680114	See	
☐	6	60006	Off-line	☒		*****				internation	680114	See	
☐	7	60007	Off-line	☒		*****				internation	680114	See	

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

Extension settings

Single Extension Add

*Extension number: DOD number:

*Registration Password Generation: ☐ Random generation ☐ Use the same password

IP Address When Using IP Authentication:

Expiration authority: Inside line

department: Please choose

CRBT: Please choose

open: ☒ Enable extension ☒ Caller ID ☐ Sound recording

Call transfer: Close

Monitor: Close

Strong interpolation: Close

function: ☐ Prohibition of substitution ☐ Call waiting ☐ Dial *33 for external calls ☐ Call hold ☐ Called switching ☐ Calling forwarding ☐ Extension message supervision ☐ Forbidden to be monitored ☐ Call Display in Call Waiting ☐ Transfer external line ☐ Call limit ☐ No forcible interposition ☐ Instant recording ☐ Extension lock ☐ Call transfer ☐ Allow phone settings to be interference-free

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.
Cryptographic	The password used for extension registration. Generate or assign a random password.
IP Address When Using IP Authentication	When the OM8000 is bi-directionally reachable with the IP address of an extension, after entering the address of the IP extension into the OM, the OM will recognize the SIP endpoint from that address as a trusted endpoint, so that the IP extension can establish a SIP session with the OM without registration.

	This function is recommended when the OM is used in conjunction with a companion voice gateway (e.g., MX120G). Fill in the IP address of the voice gateway here, and the address of the OM8000 on the voice gateway also needs to be filled into the proxy server, and set the subscriber line number of the gateway to the extension number on the OM8000.
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.
Sectoral	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, see OM User's Manual. 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 box 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 OM and the IP phone terminal are configured with a display name, the name configured on the OM 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. • Localcalls: internal 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	After entering a cell phone number, you do not need to enter a password for

Number	verification when using the *33 and *99 functions when calling into the device with that number. If the Dial *33 Outgoing 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 Outbound	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 color ringtone of the extension, please refer to the uploading and management of color ringtone files. Ringtone Upload Please refer to Uploading Color Ringtones.
(Telephone) 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 OM, 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 The specific settings of recording can be referred to.
Call Transfer	The device can transfer incoming calls to a specified phone or voice mailbox. The default is off. All Incoming Calls to Another Handset: The device transfers all incoming calls from an extension to a specified handset. 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 voice mail in case of busy/no answer: When the extension is not answering or occupied, the device transfers the incoming call to voice mail.
Distinguish Between Busy/No	When the call transfer mode is to transfer to another phone when you cannot answer , you can set the target number for busy transfer and the target number for

Answer Transfers To A Number	no-answer transfer individuallywhen Distinguish Busy/No-Answer Transfer to Number is checked.
Transfer To Number/Busy Transfer To Number/No Answer Transfer To Number	When the call forwarding mode is to 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 (Communications Link)	The device automatically calls the hotline number after taking off the machine. • Off: Turns off the Hotline function. • Immediately: The device automatically dials a pre-set hotline number immediately after taking off the phone. • Delay: If the user does not dial the number within a certain period of time after taking off the machine, the device will automatically call the hotline number. The delay time defaults to 5 seconds. The OM'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.
Stimulus 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 OM'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:

	• 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 facility's 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: Disables this extension from listening to calls from other extensions. Global: Allows this extension to listen to calls from any extension under the device. In-group only: Allow this extension to listen to the same department. Allows this extension to listen in on calls from 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.
Force Sb. To Do Sth.	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 plug blocking turned on, strong plugging does not take effect.
Prohibition Substitution	Of 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 connecting 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 hung up party. Note: Before using this feature, make sure Call Hold is turned on.
Prohibition Forced Penetration	Of 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

	displayed on the third party's phone. • Consultation Transfer: A third party (be it 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 turns: as above • Advisory referral: I bid. Note: Before using the Call Forwarding feature, make sure Call Hold, Call Forwarding is turned on.
Do Not Listen In	When this feature is turned on, calls from this extension will not be allowed to be listened to.
Caller Id On Call Waiting	The extension turns on Call Waiting, which displays the caller's number if another call comes in during the call.
Transfer To An External Line (E.G. Electric Switching)	Check this box to allow the device to allow this extension user to forward outgoing calls to a third-party cell phone or landline. Note 1: To realize the Transfer Outgoing function, the extension must also have the corresponding outgoing call authority. Note 2: When transferring an outside 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: "Drip-drip-drip-drip-drip." • Incoming external phone call: "Drip-drip-drip-drip." Incoming call from a reduced-digit dialing number: "Drip-drop-drop-drop-drop-drop-drop-drop"
Call Barring	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.

Extension Form Import

For easy configuration, OM8000 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 > Extension Form Import** to download the template and populate the information before importing.

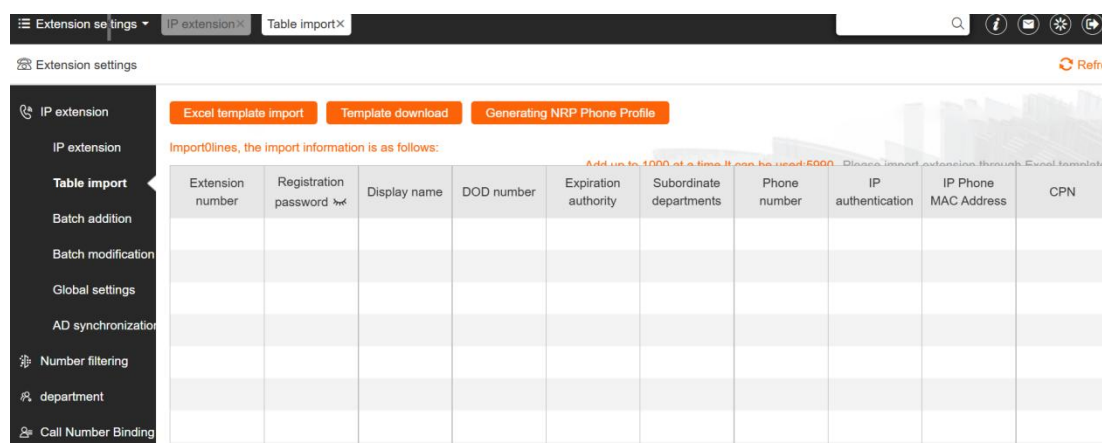


Table3-15 IP Extension Configuration Parameter Description

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 Ip Phone Configuration Files	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, OM8000 supports batch creation of extension accounts, and all extensions created in a batch have the same features enabled. If different functionality is

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

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

The screenshot displays the 'Batch addition' configuration interface. On the left is a sidebar menu with options: IP extension, Table import, Batch addition (selected), Batch modification, Global settings, AD synchronization, Number filtering, department, and Call Number Binding. The main area contains the following fields and options:

- *Initial extension number:** A text input field.
- DOD Generation Mode:** A dropdown menu with 'Use the same number' selected.
- Initial Trombone:** A text input field.
- *Lot size:** A text input field with a note: 'Add up to 1000 at a time. It can be used: 5990'.
- Registration Password Generation:** A dropdown menu with 'empty' selected.
- IP Address When Using IP Authentication:** A text input field.
- Expiration authority:** A dropdown menu with 'Inside line' selected.
- department:** A dropdown menu with 'Please choose' selected.
- CRBT:** A dropdown menu with 'Please choose' selected.
- open:** Two checkboxes: 'Caller ID' (checked) and 'Sound recording' (unchecked).
- Call transfer:** A dropdown menu with 'Please choose' selected.
- Monitor:** A dropdown menu with 'Please choose' selected.
- Strong interpolation:** A dropdown menu with 'Please choose' selected.

Extension Batch Modification

For easy modification, OM8000 supports batch modification of extensions.

Direct Modification

Click **Extension Settings > Extension 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.

Extension settings

Batch modification

Table export

Extension number: Paragraph number: Online state: whole query More screening

	Extension number	department	Display name	DOD number	Expiration authority	Registration password	IP Address When Using IP Authentication	Online state
☐	60001				international	*****		Off-line
☐	60002				international	*****		Off-line
☐	60003				international	*****		Off-line
☐	60004				international	*****		Off-line
☐	60005				international	*****		Off-line

Previous page 1 2 3 ... 39 40 41 next page Display per page

Modifying A Form After Exporting It

For easy modification, OM8000 supports batch modification of extensions by exporting Excel sheet.

Step1. Click **Extension Settings > Extension Batch Modification**.

Step2. Select the extensions that need to be modified, click **Table Export**, and check or de-select the features that need to be modified in the pop-up dialog box.

Extension settings

Batch modification

Table export

Extension number: Paragraph number: Online state: whole query More screening

export option

All election option: ☐ Expiration authority ☐ CRBT ☐ Registration Terminal IP Address ☐ IP Address When Using IP Authentication

☐ Call transfer ☐ Secretary extension ☐ Strong interpolation ☐ department

☐ Monitor ☐ Call waiting ☐ Allow phone settings to be interference-free ☐ Call hold

☐ Forbidden to be monitored ☐ Call Display in Call Waiting ☐ Call limit ☐ Extension message subscription

☐ Enable ☐ Caller ID ☐ Extension lock

Determine cancel

Expiration authority: Please choose department: Please choose Registration password: IP Address When Using IP Authentication:

CRBT: Please choose Secretary extension:

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>Global Settings** and click **OK** after setting.

► Extension global settings

Registration port: 5060 (Range: 1-9999)

Minimum registration timeout: 600 second

Minimum registration timeout after NAT: 40 second (Range: 30-65535)

SBC server:
例: 201.30.170.38:1020 或 softswitch.com:1020

Security domain: newrocktech
Used for IP Extension Registration and Authentication

Treatment of Illegal Registration: ☒ Back to 403 ☐ No response

Validity of Invitation Code: 30 Minute

Determine

Table3-16 IP Extension Parameter Description

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

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.

Figure4-6 Number Filtering Configuration Interface

Extension settings

No Outgoing Call Prefix					
1		2		3	

Table3-17 Parameter Description of Number Filtering Interface

Item	Description
Outgoing call prefixes are prohibited	Extension users are prohibited from dialing numbers with a prohibited 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 half commas ",". Note: Numbers in the Unrestricted Outbound Numbers are not subject to this restriction.
Unrestricted Outbound Numbers	Unrestricted outbound numbers are numbers that all extensions can outbound call, even if the extension is configured with outbound permissions and prohibited outbound prefixes.
Rejected caller ID	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.

4.3.2 Sectoral

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.

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

Step2. ClickSave.

Figure4-7 Department Configuration Screen

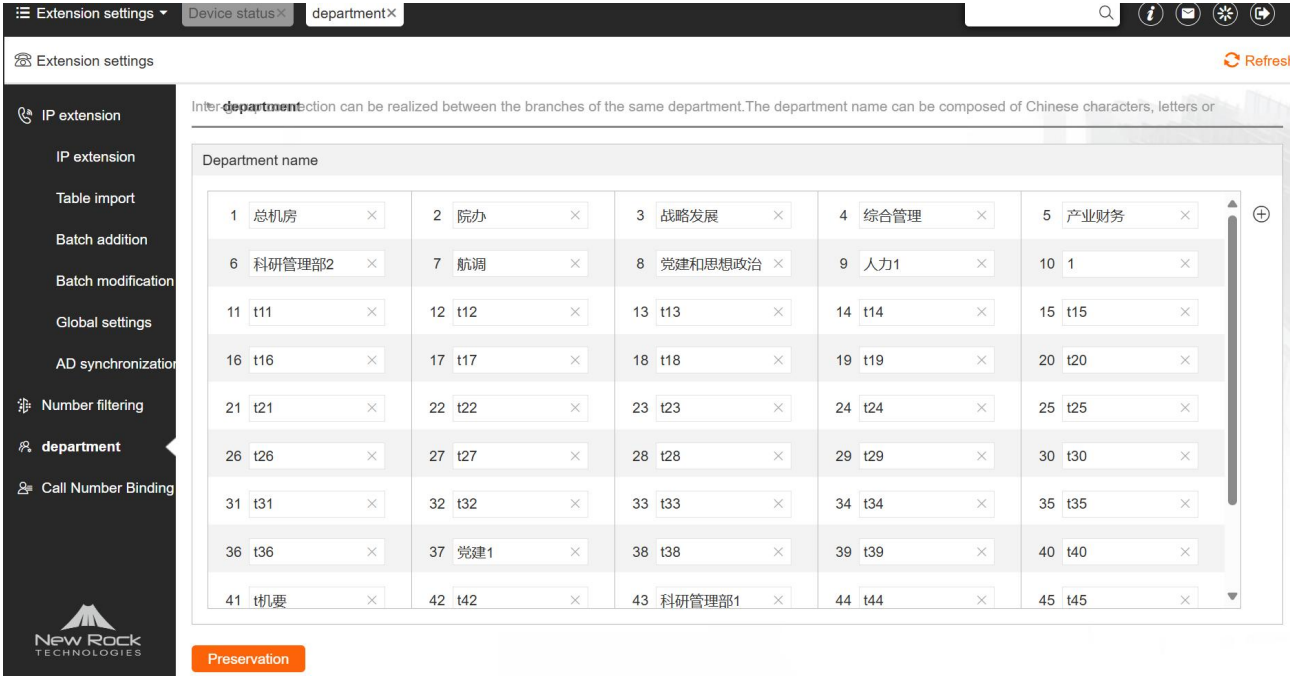


Table3-18 Parameter Description of Sectoral

Item	Description
Sectoral	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 toExtension Settings>IP Extension>IP Extensionand click thebutton. 2.Select the department to which the current extension is categorized in the Department drop-down list and clickOKto save the settings.

4.3.3 Caller ID Binding Form

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>Incoming Call Binding Numbers table** in the device interface.

Figure4-8 Incoming Call Binding Table Screen

The screenshot displays the 'Incoming Call Binding Table' interface. On the left is a dark sidebar with navigation links. The main content area has a title bar 'Call Number Binding Table'. Below it, there's a 'Get/Store Path' field containing '/var/config/bind.ini' and an orange 'Preservation' button. A 'Batch Unbinding' button is also visible. A search bar labeled 'Search number' is on the right. The central part of the screen is a table with three columns: 'Call number', 'Extension number', and 'operation'. The table is currently empty.

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 Unbinding	Batch unbinding of numbers.
Search Number	Enter the number to search. Fuzzy queries are supported.
Caller ID	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.

Item	Description
Unbundle	Individual unbinding of numbers.

4.4 External line setup

4.4.1 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 OM8000.

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.

Figure4-9 SIP Outbound New Interface

► Newly added

Relay type: Direct connection ▼

Relay Group/SIP Server:  ▼

User domain name: newrocktech.com

*number:

User name:

Password:

*Number of concurrent calls:

Access mode: Switchboard ▼

Welcome speech: Welcome Speech from OI ▼

Exhale: allow ▼

Determine **cancel**

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 OM registers to the SIP server. Registered: Remote The FXO port gateway is registered as a SIP outbound for the OM. The FXO port of the OM 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 OM.
	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 Settings > Network Configuration" interface.
	Relay Group	See.3.4.2 .
	Client 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 ID	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.
	Cryptographic	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 Method	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.
	Welcome	Select the voice navigation played by this outside line for incoming

Account Type	Item	Instructions
	Speech	calls. This item can be configured only when you select the access method as the switch board. • Switchboard Welcome Message: Indicates the use of voice navigation configured using the Basic Settings>Switch board 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 Settings>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.
	Linear Number (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 method as linear. 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.
	Breathe Out	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.

Figure4-10 SIP Outbound Configuration Interface

Outside settings

SIP external line

SIP external line

Outline table import

External batch add

Modify configuration

Registration option

Direct relay group

DOD Number Config

SIP external line

number: Paragraph number: Registration status: whole

No screening conditions

Newly added delete Delete all if no item selected SIP Outer Line Number Available: 7498 SIP Outline Number Used: 502

	line	Relay type	Registra status	number	Number of concurre calls	Use nam	Pas	depa	SIP server	Use dom nam	Acco mod	Welk spec	Line num (DID)	Exhale	Sound recording
☐	8001	Direct c	unregist	86830000	2	868			--	new	stra		300	Share	Not allow
☐	8002	Direct c	unregist	86830000	1	868			--	new	stra		300	Share	Not allow
☐	8003	Direct c	unregist	86830000	1	868			--	new	stra		300	Share	Not allow
☐	8004	Direct c	unregist	86830000	1	868			--	new	stra		300	Share	Not allow
☐	8005	Direct c	unregist	86830000	1	868			--	new	stra		300	Share	Not allow

Table3-21 SIP Outbound 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. - Not registered, 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 theApplication Services>Recording page For details, see 3.5.3 .
Removing	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.

SIP external line

number:		Paragraph number:		-		Registration status:	whole	▼
---------	----------------------	-------------------	----------------------	---	----------------------	----------------------	-------	---

Outside Forms Import

For easy configuration, OM8000 supports batch import of multiple SIP outside accounts via Excel (up to 1000 SIP outside accounts at one time).

Step1. Click **Outbound Settings>SIP Outbound>Outbound Form Import**.

Step2. Click on the **template to download it**.

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.

[Excel template import](#)
[Template download](#)
Add up to 1000 at a time. It can be used: 7498
Please import SIP Outline through Excel template.

Import 0 lines, the import information is as follows:

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

External Batch Addition

To simplify the configuration, OM8000 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 Outbound> 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**.

Outside settings

SIP external line

Outline table import

External batch addition

Modify configuration

Registration option

Direct relay group

DOD Number Configuration

New Rock TECHNOLOGIES

Batch addition

Relay type: Direct connection

*Initial Registration Account:

*Number of concurrent calls:

*Lot size: Add up to 1000 at a time. It can be used: 7498

Registration Password Generation: empty

Relay Group/SIP Server:

proxy server:

User domain name:

Local Port Generation: Using local ports

Access mode: Switchboard

Welcome speech: Welcome Speech from O

Determine

Outside line Batch modification

For easy modification, OM8000 supports batch modification of external line configuration.

Click **Outbound Settings > SIP Outbound > 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 to modify the configuration. Click **OK**.

Outside settings

SIP external line

Outline table import

External batch addition

Modify configuration

Registration option

Direct relay group

DOD Number Configuration

New Rock TECHNOLOGIES

Modify configuration

number: Paragraph number: Registration status: whole

query More screening

	Relay type	Registration status	number	Number of concurrent calls	User name	Password	SIP server	User domain name	Access mode	Welcome speech	Line number (DID)	Exhale	Sound recording
☐	Direct connect	unregistered	86830003	1	86830003		--	newrocktech.c	straight line		30003	Share	Not allow
☐	Direct connect	unregistered	86830004	1	86830004		--	newrocktech.c	straight line		30004	Share	Not allow
☐	Direct connect	unregistered	86830005	1	86830005		--	newrocktech.c	straight line		30005	Share	Not allow
☐	Direct connect	unregistered	86830006	1	86830006		--	newrocktech.c	straight line		30006	Share	Not allow
☐	Direct connect	unregistered	86830007	1	86830007		--	newrocktech.c	straight line		30007	Share	Not allow
☐	Direct connect	unregistered	86830008	1	86830008		--	newrocktech.c	straight line		30008	Share	Not allow

Previous page 1 2 3 ... 9 10 11 next page Display per page

Number of concurrent calls:

Access mode: Please choose

Exhale: Please choose

Sound recording: Please choose

Relay type: Please choose

Local Port Generation: Please choose

Determine Reset

Registration Options

Click **Outbound Settings > SIP Outbound > 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.

Figure4-11 SIP Outbound Registration Options Screen

The screenshot displays the 'Registration options' configuration page. The left sidebar contains navigation links: 'SIP external line', 'Outline table import', 'External batch add', 'Modify configuration', 'Registration options' (selected), 'Direct relay group', and 'DOD Number Config'. The main content area includes the following fields:

- Default Register Server:** Text input with example: 168.33.134.51:5000 or www.sipproxy.com:5000
- Local port:** Text input with value 5060 and range: 1-9999, default: 5060
- Registration timeout:** Text input with value 600 and range: 15-86400, default: 600
- proxy server:** Text input with example: 168.33.134.51:5000 or www.sipproxy.com:5000
- Switching Local Port Increments:** Dropdown menu with value 0
- Register multiple platforms:** Dropdown menu with value Close
- User domain name:** Text input with value newrocktech.com
- Subdomain name:** Text input
- SIP contact header domain address type:** Radio buttons for LAN address and WAN address (WAN is selected)
- SDP C Header Domain Address Type:** Radio buttons for LAN address and WAN address (WAN is selected)
- Backup mode:** Dropdown menu with value Close
- IMS:** Dropdown menu with value Close
- Limit SIP Outline Concurrency:** Text input with value 0

A 'Determine' button is located at the bottom right of the configuration area.

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 Settings > 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 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.
Transforms The Local Port Incremental Value	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 For 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.
Client Domain Name	The attribution of the IP outbound number, provided by the SIP outbound carrier, example: abccompany.com.
Subdomain	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 Field 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 Cheader Field 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. • 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: a 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: A 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.
Limit The Number Of Concurrent Sip Outside Lines	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.

4.4.2 Directly Connected Repeater Group

This function is used in conjunction with the New Rock MX100G Trunk Gateway. After the configuration is completed, all SIP outbound calls will be outbound from the MX100G.

Step1. Click **Outside Line Settings>SIP Outside Line>Direct Connect Trunk Group**.

Step2. Click **Add** and fill in the two server addresses (i.e., the addresses of the two MX100Gs, which will automatically switch to the other if one has connection problems).

	Group number	Group call restrictions	Hunting Mode	Server 1	Server 2	Server 3	operation
☐							

Step3. Click **Outside Line Settings>SIP Outside Line**, set the trunk type of the outside line to **Direct Connection**, and select the trunk group configured in the previous step for the **trunk group/server**.

Group number: 1

Group call restrictions:

Hunting Mode:

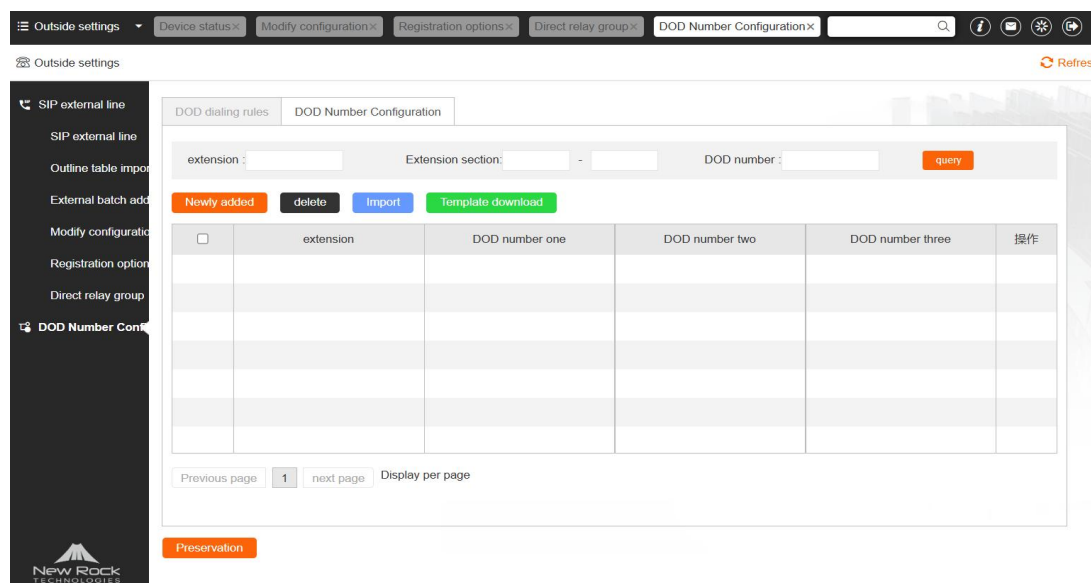
The server	IP address	Call restrictions	Primary server	Standby server
The server1			☐	☐
The server2			☐	☐
The server3			☐	☐
The server4			☐	☐
The server5			☐	☐
The server6			☐	☐
The server7			☐	☐
The server8			☐	☐

Preservation

4.4.3 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.

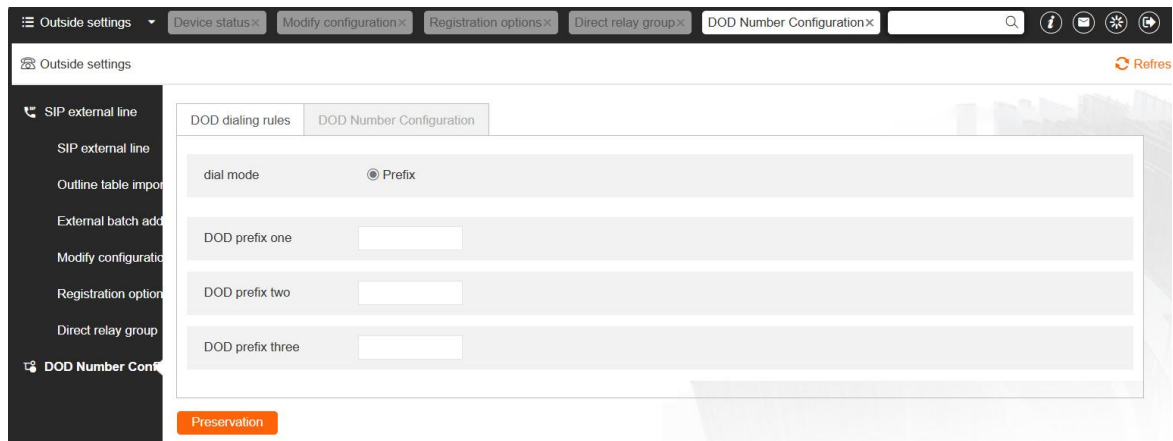
If you need to configure bound outside numbers for a large number of extensions, we recommend you to click "Template Download", then edit the template and click "Import". A screenshot inside the template `dod_import_template.xlsx` is shown below:

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.

Figure4-12 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.

4.5 Application Service

4.5.1 Media, Esp. News Media

Go to **Application Services>Media** to configure Voice over IP media parameters.

Figure4-13 Media Configuration Interface

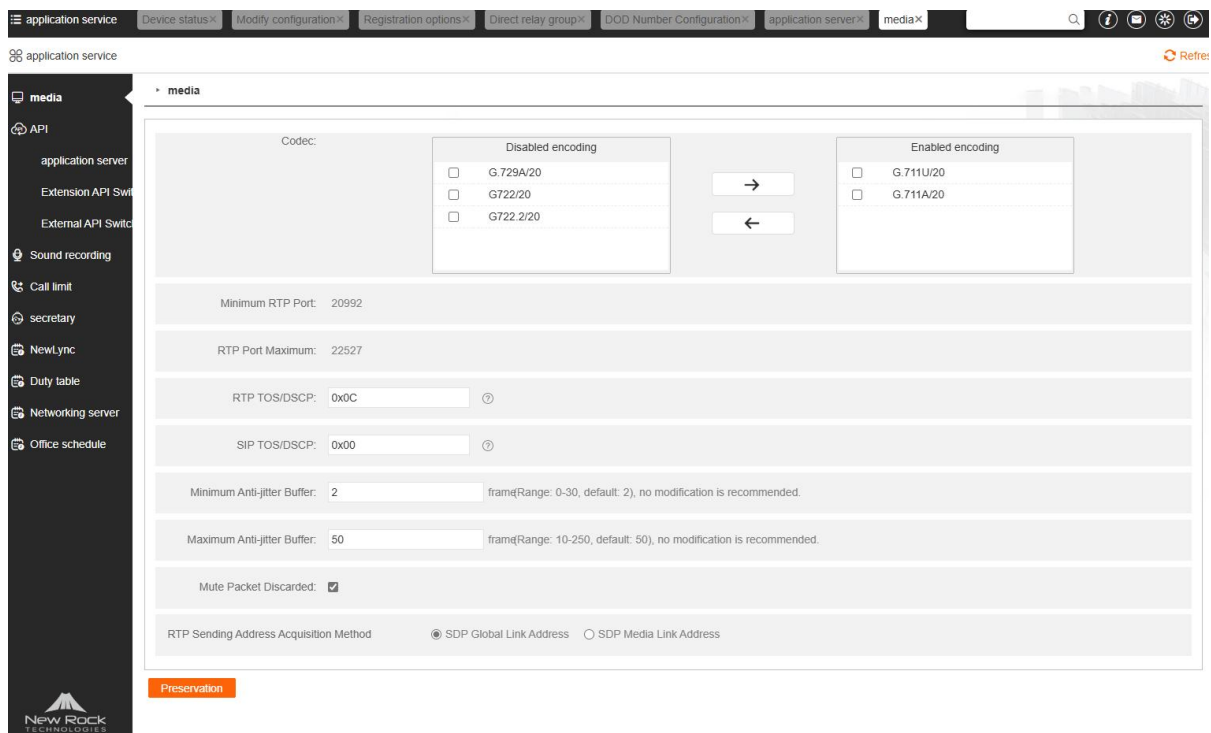


Table3-23 Description of media parameters

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.
Anti-Dithering Buffer Min.	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.
Anti-Flicker Buffer Max.	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.
Silent Packet Discard	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 Send 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).

4.5.2 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 Services > API** and fill in the API server address (i.e. the address

of the external application).

Figure4-14 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 OM only recognizes API request messages from this IP address, and when the OM 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 Signed Authentication Password (Receive)	The OM only receives API request messages from authenticated application servers. After configuring the OM digital signature authentication password, the key assigned on the application server needs to be consistent with the one configured here.
Digitally Signed Authentication Password (Sent)	The OM 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.
Digital Signature Validity	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.

Extension API Switch

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

The screenshot displays the 'Extension API Switch' configuration page. At the top, there are search filters for 'Extension number' and 'Paragraph number', and a 'Condition monitoring' dropdown set to 'Please c'. A 'query' button is present. Below the filters is a table with three columns: a checkbox column, an 'Extension number' column, and a 'Condition monitoring' column. The table lists extension numbers from 60001 to 60011. The 'Condition monitoring' column shows checkboxes, all of which are currently checked. At the bottom of the table, there are pagination controls: 'Previous page', '1', 'next page', and 'Display per page'. A 'Presen' button is located at the bottom left of the page.

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.

Outside API switch

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

The screenshot shows the 'Extension API Switch' configuration page. The left sidebar contains a menu with options like 'API', 'application server', 'Extension API Switch', 'External API Switch', 'Sound recording', 'Call limit', 'secretary', 'NewLync', 'Duty table', 'Networking server', and 'Office schedule'. The main content area has a search bar with 'Extension number' and 'Paragraph number' fields, and a 'Condition monitoring' dropdown. Below the search bar is a table with columns for 'Extension number' and 'Condition monitoring'. The table lists extension numbers from 60001 to 60011, all with 'Condition monitoring' checked. The interface includes buttons for 'open', 'Close', 'query', and 'Reset'.

Extension number	Condition monitoring
60001	☒
60002	☒
60003	☒
60004	☒
60005	☒
60006	☒
60007	☒
60008	☒
60009	☒
60010	☒
60011	☒

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 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 calls from this outside line before answering.
Incoming Answering 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.

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

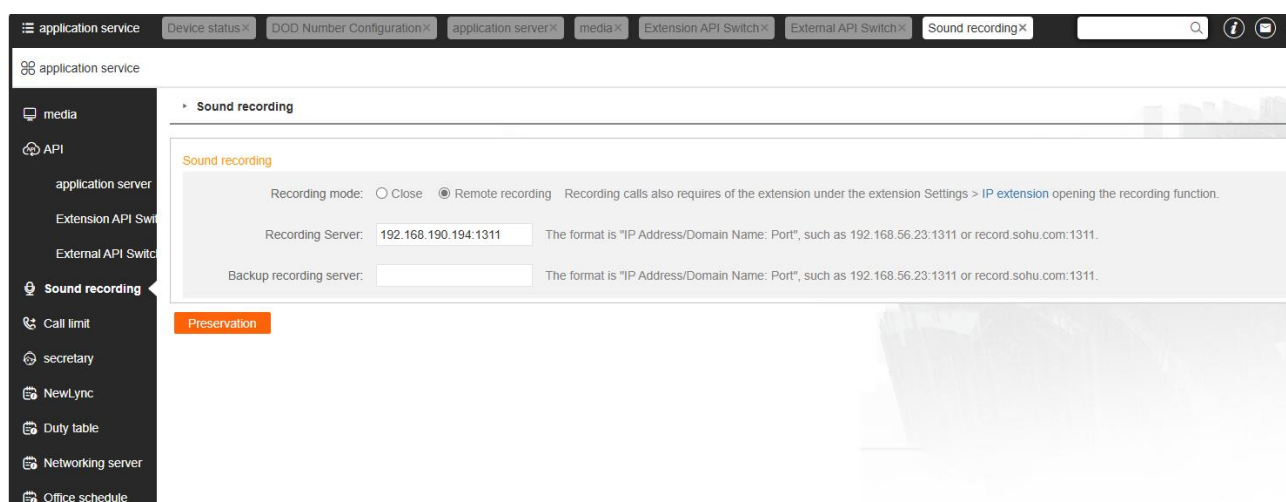
4.5.3 Sound Recordings

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 New Rock "Full Record" recording agent software or the New Rock recording management system.

The configuration steps are as follows:

Step1. Click **Application Services>Recording** and select **Remote Recording**.

Figure4-15 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 **Recording** in the Extension function.

Figure4-16 Extension Recording Configuration Interface

More screening

Enable:

Please choose

DOD number:

department:

Please choose

Display name:

Expiration auth
ority:

Please choose

At the end of th
e number is:

function:

☐ Prohibition of substitut
☐ Call waiting
☐ Allow phone settings to be changed
☐ Call transfer-free

☐ Calling forwarding
☐ Extension message su
☐ Forbidden to be monitored
☐ Call Display in Cal

☐ Transfer external line
☐ Call limit
☐ Caller ID
☐ No forcible interpo

☐ Extension lock
☒ Sound recording
☐ Instant recording
☐ Dial *33 for extern

Determine

cancel

Step6. Click **OK**.

Note: To manage recorded files (audition, search, delete, etc.) on the recording server, please refer to the [All Recording Agent Software User's Guide](#) or [Timeless Recording Management System User's Manual](#).

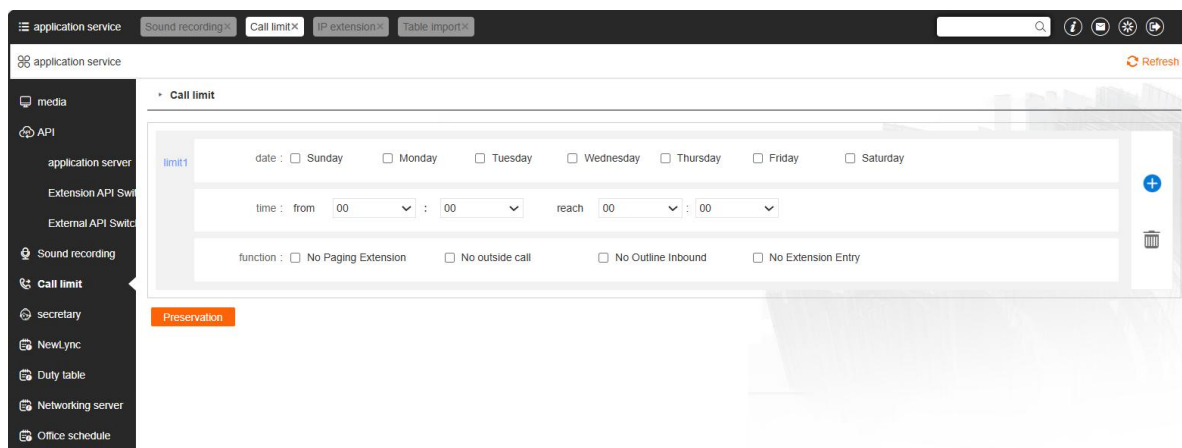
4.5.4 Call Barring

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 Services>Call Restriction** 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.

Figure4-17 Call barring configuration screen



Step3. **Save** the settings.

Step4. Go to **Extension Settings>IP Extension**, click the corresponding action icon of the extension.  Click on the icon corresponding to the extension, and check the **call restriction** function of the extension.

Step5. **Save** the settings.

4.5.5 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.

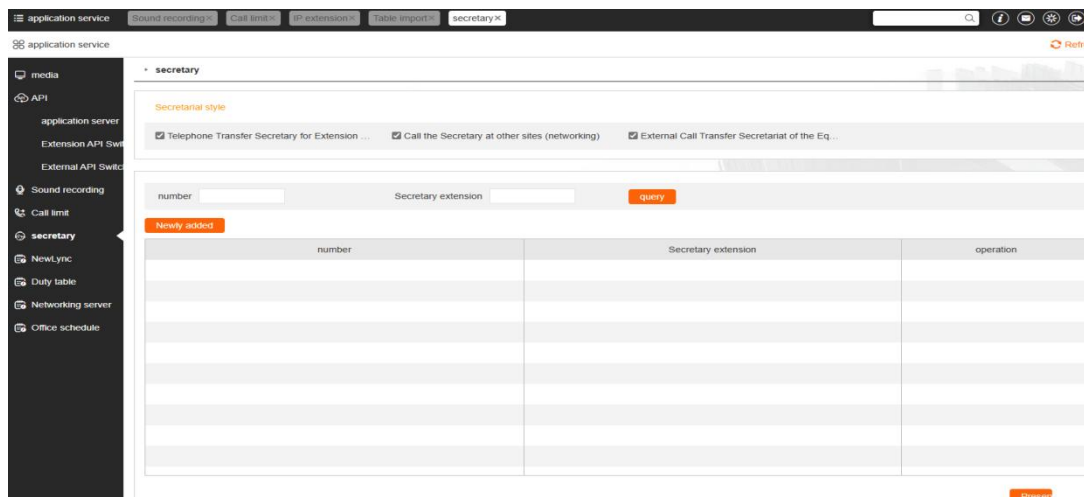


Table3-27 Outside API switch Parameter Description

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 facility's 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**.

4.5.6 Duty Roster

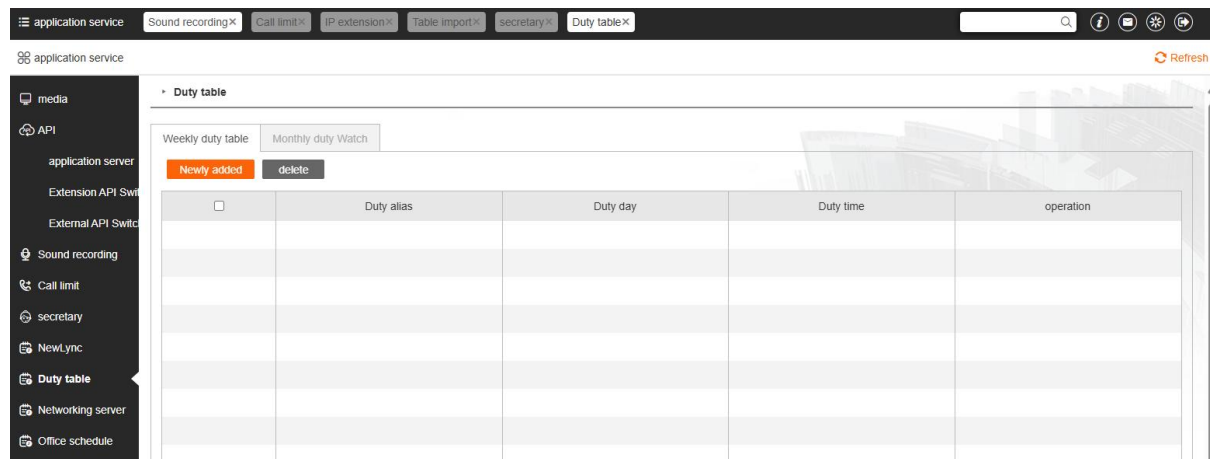
The Duty List is used to configure the duty officer who answers incoming calls from outside the facility during non-working hours. This function is divided into two ways: weekly duty and monthly duty.

Step1. Go to **Application Services>Duty List**.

Step2. Select the mode of duty.

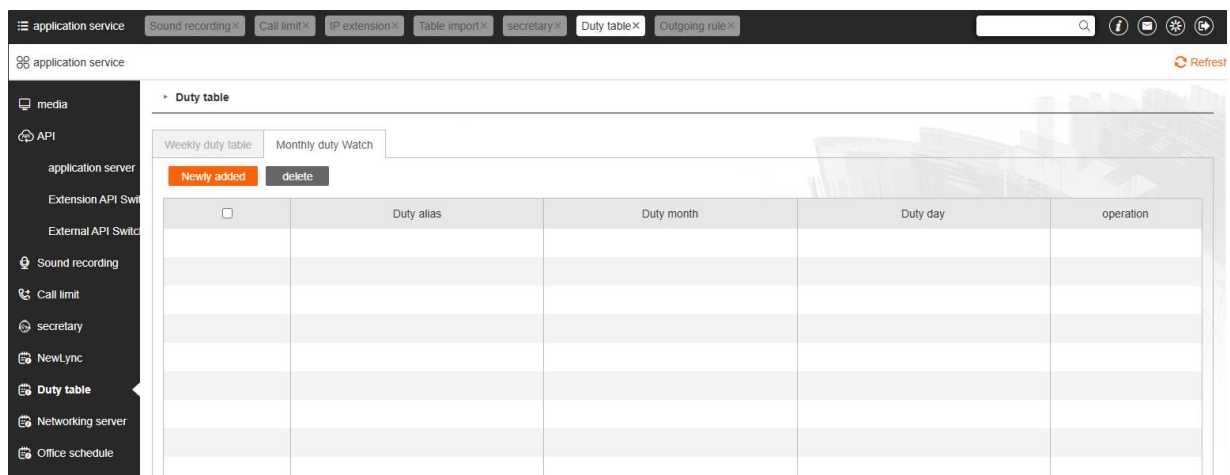
Weekly duty roster

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

Click **Add** to enter the Weekly Duty List Configuration screen, as shown below.

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

Duty day	Type of on-duty telephone	Watchman	Duty number
1			
2			
3			
4			
5			
6			
7			

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".
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 the Basic Settings>Switchboard page.
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 the name displayed in 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

Click **Add** to enter the Monthly Duty List Configuration screen, as shown below.

After completing the settings, click **Save**. Monthly duty schedules are in effect for the designated month.

Monthly Duty Schedule - Added

Duty alias: prefix:

Outside lines: Duty month:

Duty number

Duty day	Type of on-duty telephone	Watchman	Duty number
1			
2			
3			
4			
5			
6			
7			

Preservation

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 the Basic Settings>Switchboard page.
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 the name displayed in 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

Item	Instructions
	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.

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 in **Extension Settings>IP Extension**.

Step3. Create a weekly duty roster at **Application 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.

The screenshot shows the 'Weekly Duty Schedule - Added' configuration page. The interface includes a sidebar with various service options like media, API, application server, and 'Duty table' (which is selected). The main content area has fields for 'Duty alias' and 'prefix', a dropdown for 'Outside lines', and a link for 'Duty time interval'. Below these is a table for 'Duty number' with columns for 'Duty day', 'Type of on-duty telephone', 'Watchman', and 'Duty number'. The table rows correspond to the days of the week from Monday to Sunday. A 'Preservation' button is located at the bottom right of the table.

Duty day	Type of on-duty telephone	Watchman	Duty number
Monday			
Tuesday			
Wednesday			
Thursday			
Friday			
Saturday			
Sunday			

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.

This screenshot shows the 'Weekly Duty Schedule - Editor' page, which is identical in layout and content to the previous 'Added' page. It features the same sidebar, configuration fields for 'Duty alias', 'prefix', 'Outside lines', and 'Duty time interval', and the same 'Duty number' table with columns for 'Duty day', 'Type of on-duty telephone', 'Watchman', and 'Duty number'. A 'Preservation' button is also present at the bottom right.

Duty day	Type of on-duty telephone	Watchman	Duty number
Monday			
Tuesday			
Wednesday			
Thursday			
Friday			
Saturday			
Sunday			

4.6 Advanced Settings

4.6.1 Systems

Site attribution area code

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

Figure4-18 Attribution area code configuration screen

advanced setting

Switchboard>

IP extension>

Network management>

Duty table>

system>

advanced setting

Refresh

Call black/white list

system

certificate

Function code

Dial detection

SIP compatibility

Routing table

Network management

Geo-redundant

system

Native domain name:

Number of rings triggering unanswered transfer: 3 second (Scope: 0-255)

Site Attribution Area Number

National Area: China Local area code:

DTMF

transmission mode: RFC2833 2833Load type: 101 (Range: 96-127 default: 101)

Range setting

Extension number ran... -

Extension Number Ra... -

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 toAdvanced Settings>Systemto configure DTMF information.

Figure4-19 DTMF interface

DTMF

transmission mode: RFC2833

2833Load type: 101 (Range: 96-127 default: 101)

Table3-32 DTMF Parameter Description

Item	Instructions
transmission method	The transmission methods of DTMF signals supported by the OM 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. Click**Save**.

4.6.2 Certificates

Go to**Advanced Settings>Certificates**, click**Upload**, select the certificate and upload it.



4.6.3 Function Code

Click**Advanced Settings>Function Code**to 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.

Figure4-20 Function Code Configuration Screen

Function code configuration screen details:

- system**
 - Query IP Address: ##
 - Inquiry Extension Number: #00
 - Setting IP Address: *90
 - Modify extension number: *96
- Voice prompt recording**
 - Recording: *81
 - Audition: *82
 - Preservation: *83
- Business operation**
 - Call Park: *30
 - Substitute switchboard: *50
 - Password outgoing: *33
 - Monitor: *34
 - Strong interpolation: *39
 - Call binding: *67
 - Call Residence Retrieval: #30
 - Replacement of designated extensi: *55
 - Blind turn: *38
 - Instant recording: *#
 - Listen to Language Messages: *98
 - Wake up: *36
 - Substitute any extension: *51
 - Substitute intra-group extension: **71
 - Three party call: *79
 - Call back when called in a hurry: *31
 - Incoming call binding: *66
 - Common Functional Navigation: *99

Business enabled

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**

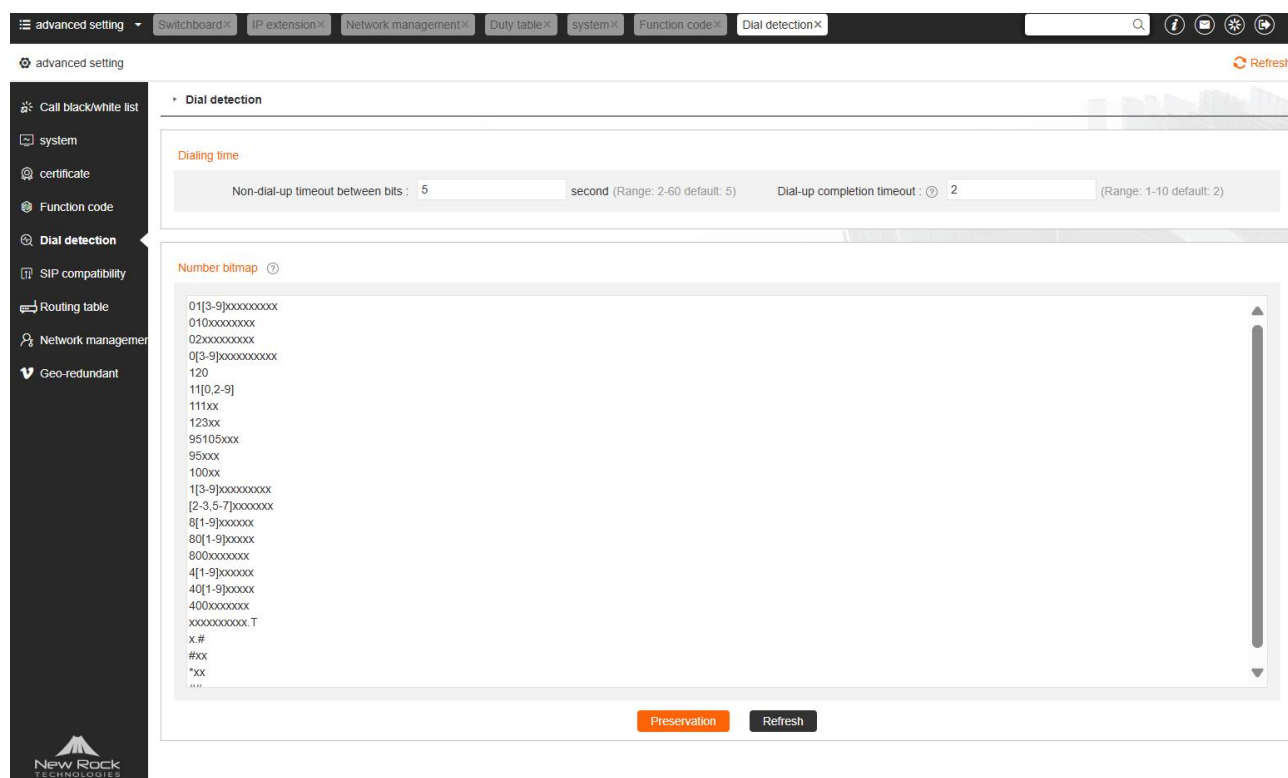
Feature codes cannot conflict with extension numbers, group numbers of call answering groups, transferring switchboard numbers, outgoing call selector prefix numbers and other feature codes.

4.6.4 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.

Click **Advanced Settings** > **Dial Detection**, set the rules related to the number bitmap and click **Save**.

Figure4-21 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 "XXXXXXXXXXXX.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).
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".
xxxxxxxxxxxx.	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.
02xxxxxxxxx	Receiving an 11-digit number starting with 02 ends the collection. Used to define long distance calls beginning with 02.
013xxxxxxxxx	Receiving a 12-digit number starting with 013 ends the collection. Used to define long distance cell phone calls that begin with 013.
13xxxxxxxxx	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.

4.6.5 SIP Compatibility

Step1. Go to **Advanced Settings > SIP Compatibility** to set the SIP compatibility information.

Figure4-22 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 when Early Media is 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.
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

Item	Instructions
	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".
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

Item	Instructions
	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**.

4.6.6 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 to **Advanced Settings>Routing Table** to add routing rules.

Specific instructions are given below.

Number Conversion

Figure4-23 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

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 calls from IP 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. Click **Add to Routing Table**.

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

3. Finally, click **Save**.

The screenshot displays a web interface for configuring a routing table. At the top, there is a tab labeled "Routing table" with an "Explain" link. Below the tab is a table with three columns: "Number change", "Call time limit", and "Route". The "Route" column is currently selected. Below the table, there are three sections: "Outgoing line", "Called number matching", and "Add Number Prefix". The "Outgoing line" section shows "IP external line" and a dropdown menu with "Choose routes or input routes se". The "Called number matching" section has two radio buttons: "Arbitrary number" and "Specified number", with "Specified number" selected. The "Add Number Prefix" section has a text input field labeled "Input number or prefix" and another labeled "Please enter number prefix". An orange button labeled "Adding Routing Table" is positioned below these sections. At the bottom right, there is a "Switching display mode" button.

Outgoing Time Limit

Figure4-24 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.

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.

Configuration method:

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

1. Click **Add to Routing Table**.

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

3.Finally, clickSave.

advanced setting

Dial detection SIP compatibility Routing table

advanced setting

Call black/white list system certificate Function code Dial detection SIP compatibility Routing table Network management Geo-redundant

Routing table

Number change Call time limit Route

Called prefix

Call duration (minutes)

Please enter a prefix or number to limit

Please enter the call duration

Adding Routing Table

Routing table

Switching display mode

Preservation

New Rock Technologies

Directional Routing

advanced setting

Dial detection SIP compatibility Routing table

advanced setting

Call black/white list system certificate Function code Dial detection SIP compatibility Routing table Network management Geo-redundant

Routing table

Number change Call time limit Route

Call source

IP extension

Number matching

Arbitrary number Specified number

Send to

IP external line

Choose routes or input routes se

Input number or prefix

Please click the button on the right t

Adding Routing Table

Routing table

Switching display mode

Preservation

New Rock Technologies

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

Item	Description
	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 the specified 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 the **call 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.

Finally, click **Save**.

4.6.7 Network Management

EMS

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

Step2. Click **Save**.

TR069

Step1. Go to **Advanced Settings>Network Management**and select TR069 to configure.

Figure4-25 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.

Item	Description
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 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**.

SNMP

Step1. Go to **Advanced Settings>Network Management** to configure it.

Figure4-26 SNMP Configuration Interface

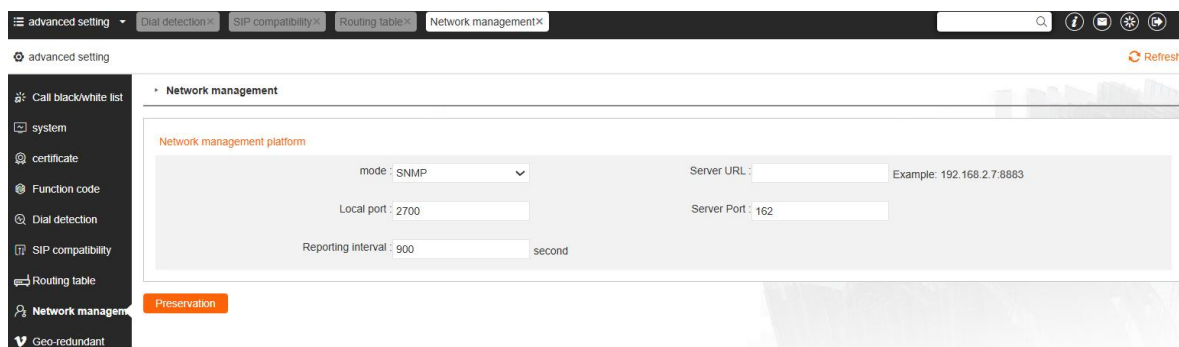


Table3-40 SNMP Parameter Description

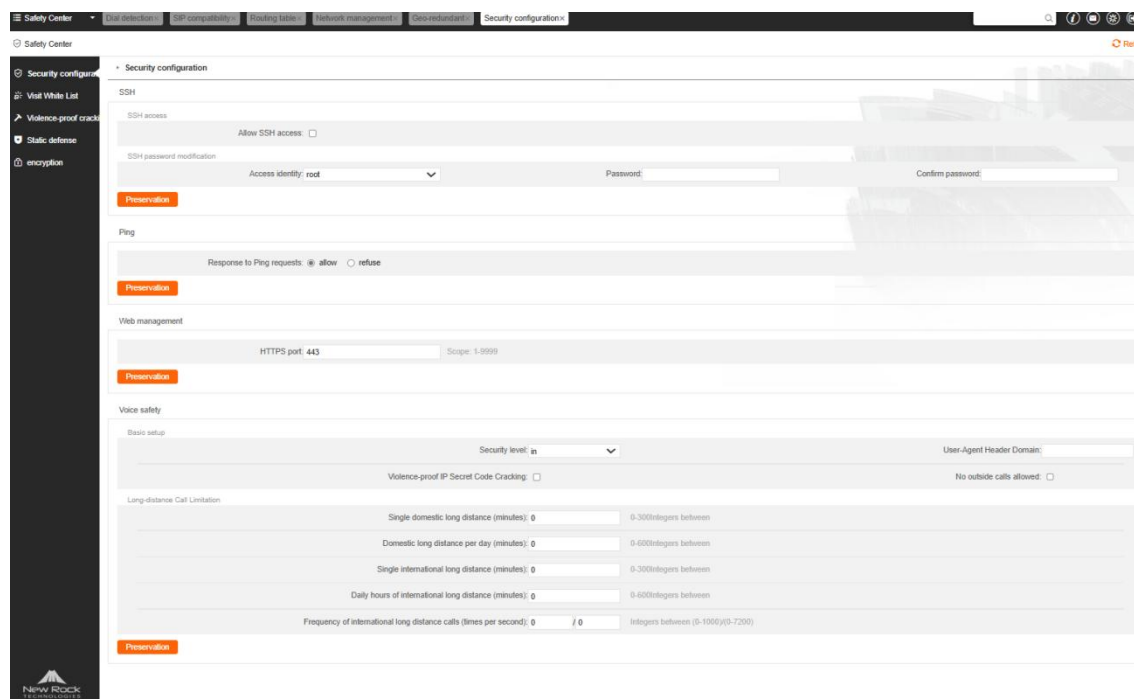
Item	Description
Server URL	Set the URL of the webmaster server.
local port	Enter the SNMP local port. The default is 2700. If you select the SNMP method, you need to fill in the following three parameters.
server (computer)	Enter the SNMP server address.
server port	Enter the SNMP server port number.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

Step2. Click **Save**.

4.7 Security Center

4.7.1 Safety Configuration

Go to **Security Center>Security Configuration**.



SSH

Go to **Security Center>Security Configuration** and 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.
Password /	Change the root user/operator user password for SSH access. Passwords are

Item	Description
Confirm Password	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

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

Figure4-27 Web Management Configuration Interface

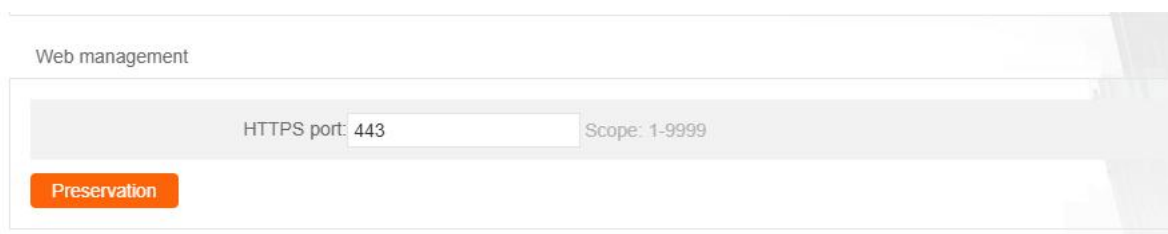


Table3-43 Web Management Interface Parameter Description

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.

Figure4-28 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 OM is restarted.
Long Distance Call Restriction	

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.

4.7.2 Access To A White List

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

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

The configuration steps are as follows:

Step1. Go to **Security Center>Access Whitelist**, click **Add**, and fill in the whitelist information. The device can add up to 20 addresses.

Figure4-29 Whitelist Configuration Screen

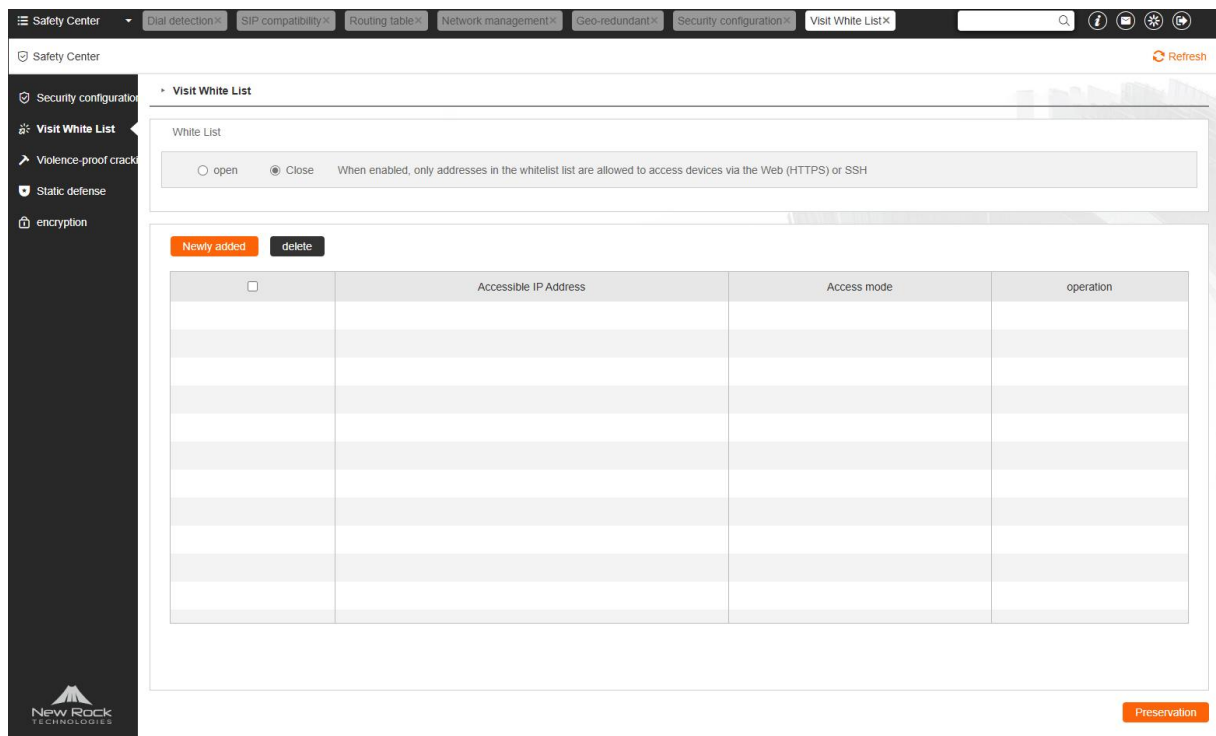


Table3-45 Description of whitelisting parameters

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 on**whitelisting.



Note

To access the device via SSH, you also need to enable the SSH service for the device on the **Security>Security Configuration** page.

4.7.3 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, click **Security Center>Anti-Violence Breach Accounts** to open this configuration screen.

Figure4-30 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.
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

Item	Description
	default is 10 minutes.

Locked list

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

Figure4-31 Anti-brute-force account (lock list) screen

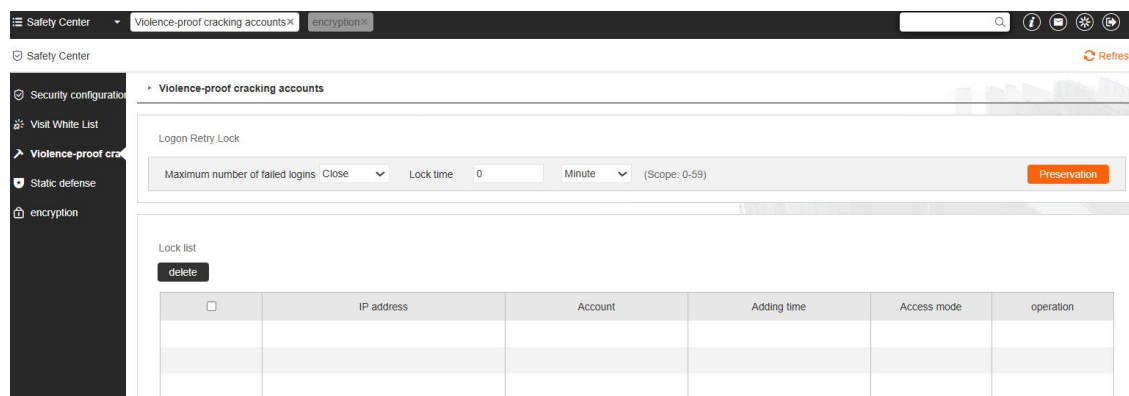


Table3-47 Anti-brute-force account (lockout list) display information

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.

4.7.4 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, click **Security Center>Static Defense** to open this configuration screen.

Figure4-32 Static Defense Configuration Interface

[illegible]

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.



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

2. typical example

☒	Local port	Source IP address	Permission/Prohibit	Agreement	operation
☒	5060-5061	192.168.120.54	prohibit	tcp	

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).

4.7.5 Encrypted

Go to **Security Center>Encryption** to open this screen.

Figure4-33 Cryptographic Interface

encryption

Signal Encrypt ☐ open ☒ Close

Encrypted object ☐ IP extension ☐ SIP external line ☐ networking

Encryption mode Use UDP protocol to encapsulate signaling and RTP data with ei

Voice Packet Encryption No encryption (0)

T.38 Data Encryption ☐ open ☒ Close

encryption key

SBC

SBC address Example: 201.30.170.38:1020 or softswitch.com:1020

Local port 4660 (Range: Port range cannot be 20992 ~ 22527)

Preservation

Table3-49 Description of encryption parameters

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

Item	Description
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 the Basic Configuration > Network interface. For example: 201.30.170.38:1020 or softswitch.com:1020.
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.

4.8 System Maintenance

4.8.1 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 to **System 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.

4.8.2 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

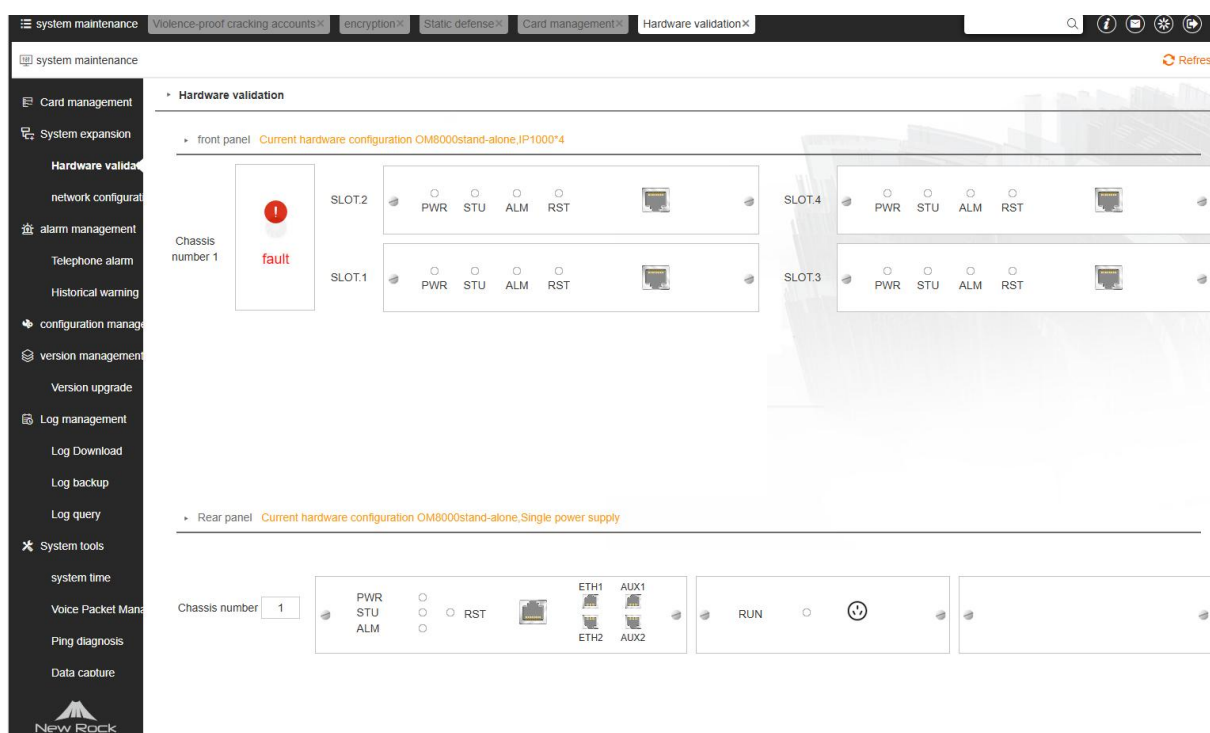
Go to **System Maintenance > System Expansion > Hardware Confirmation**.

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.

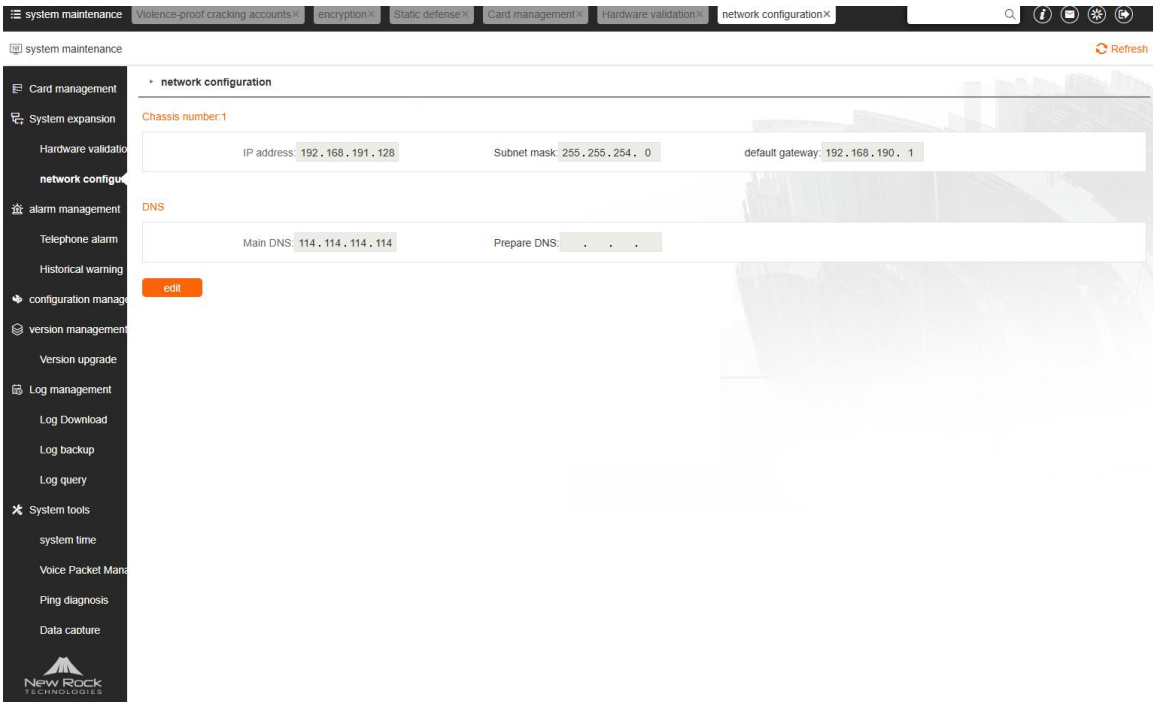
When the new chassis is connected properly, the system will detect it and prompt "New machine found" on the page.

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



Step2. network setup

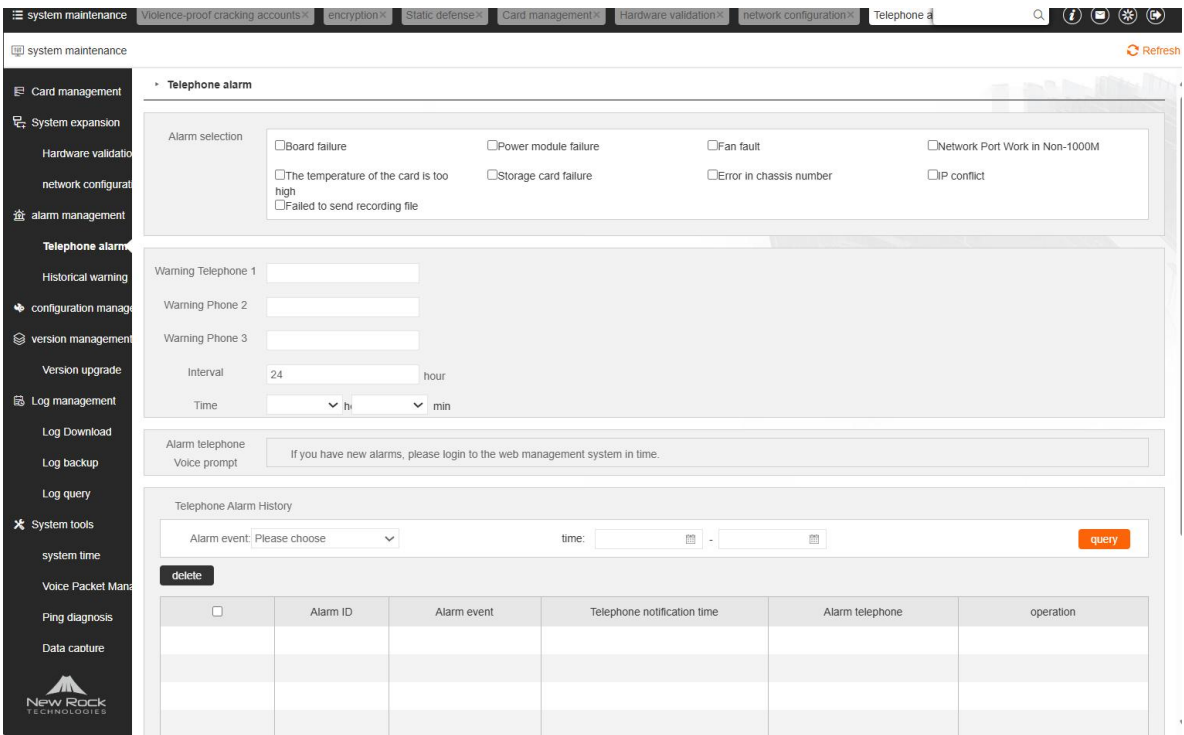
Go to **System Maintenance>Network Configuration>Edit** to configure the network parameters for the added chassis and the entire machine.



4.8.3 Alarm Management

Telephone alarm

Go to the **System Maintenance > Phone Alarms** page to configure the phone number and phone alarm category to answer the alarm.



Alarm History

Go to the **System Maintenance > Historical Alarms** page to view historical alarm information and to acknowledge and eliminate alarms.

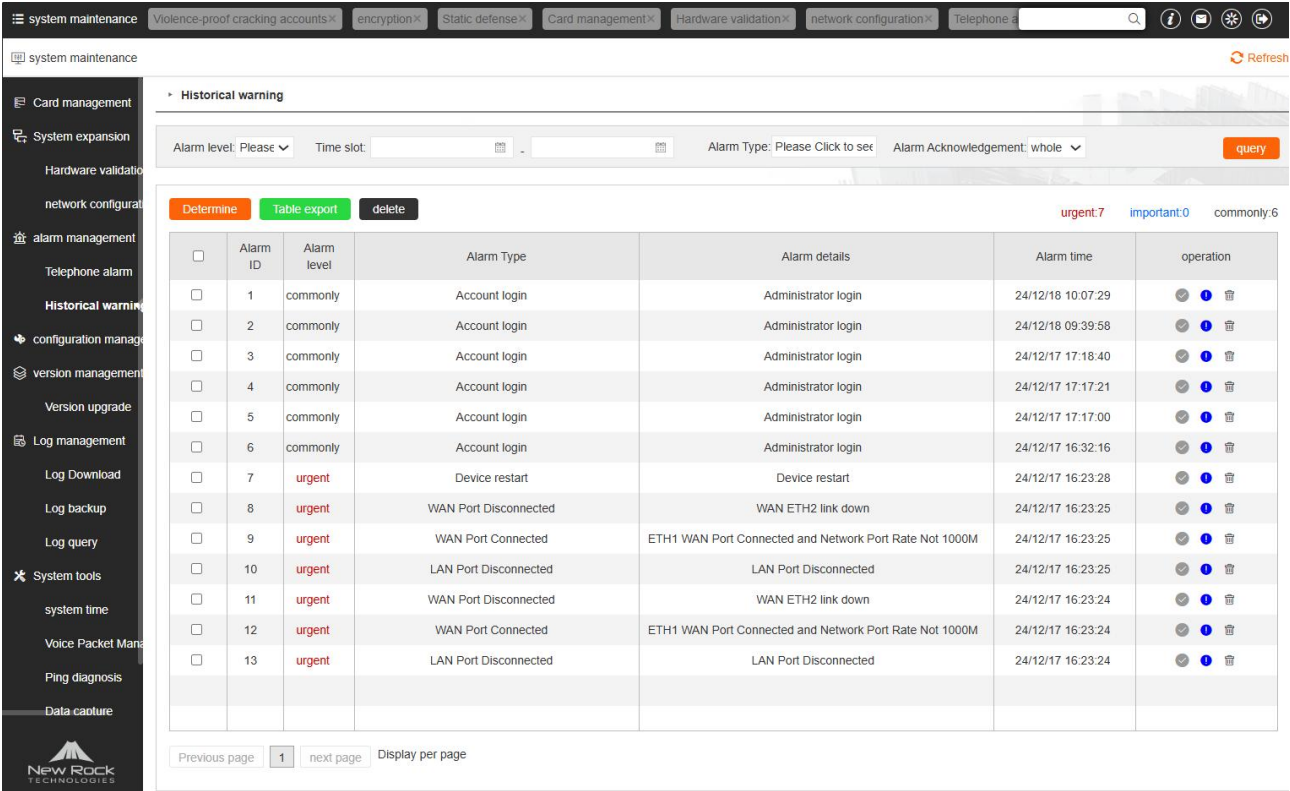


Table3-51 Classification of alarm messages

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

form	element
	New card detected
	Discover the new OM8000 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
	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

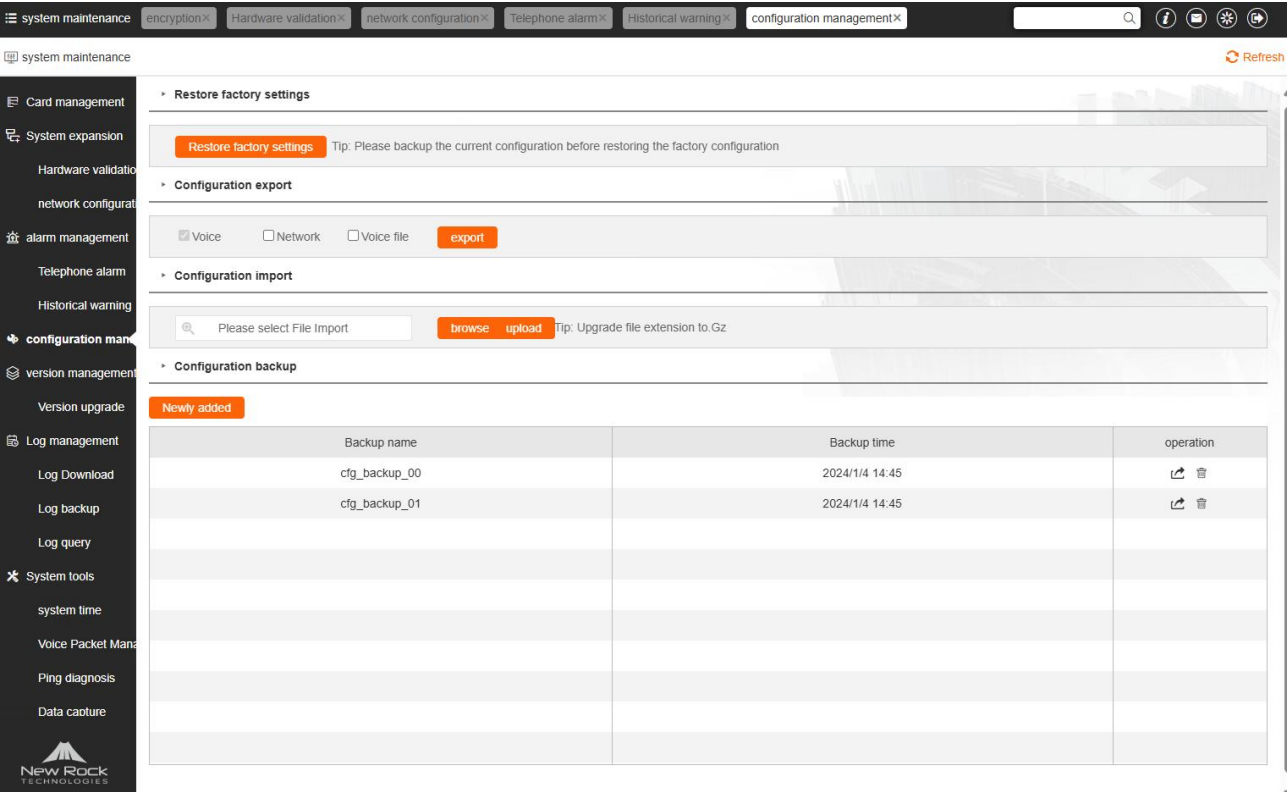
form	element
	Dual-computer cascade not connected
	IP conflict

4.8.4 Configuration Management

Go to **System Maintenance>Configuration Management**to 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.





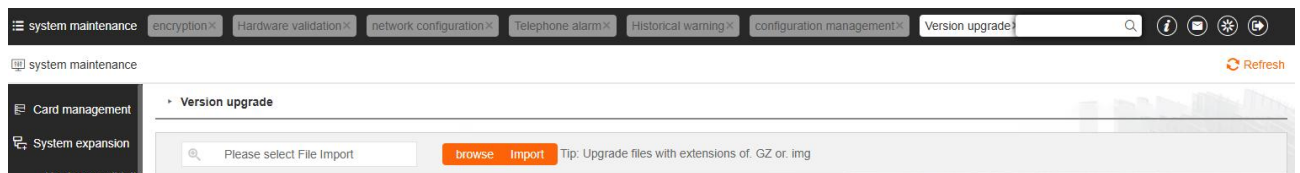
Note

- 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.

4.8.5 Version Management

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

Figure4-34 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.

4.8.6 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 click **Download** to download the logs.

Figure4-35 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.
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 to **System Maintenance > Log Management > Log Backup**, set the FTP server address and user name and password, and the logs will be backed up automatically.

The screenshot shows the 'Log backup' configuration page. The left sidebar lists various system maintenance options, with 'Log backup' selected. The main content area has two sections: 'FTP backup' and 'NAS backup'. Each section has an 'Enable' checkbox and input fields for 'FTP address', 'port', 'User name', and 'Password'. The 'FTP backup' section is currently active. A 'Refresh' button is visible in the top right corner of the main content area.

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
cryptographic	Fill in the password set on the FTP server

4.8.7 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.

Click **System Maintenance > System Time** to configure the time server.

Figure4-36 System Time Configuration Screen

▶ system time

time zone: (GMT+08:00) Beijing

Current time: 2024-12-18 11:20:22

Time calibration

Preferred time server: 198.60.22.240

Standby time server: 133.100.9.2

System time synchronization interval: 120

Minute

Preservation

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 click Clock Calibration to 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.
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 the**Clock Calibration**button 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, see Table3.56.

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

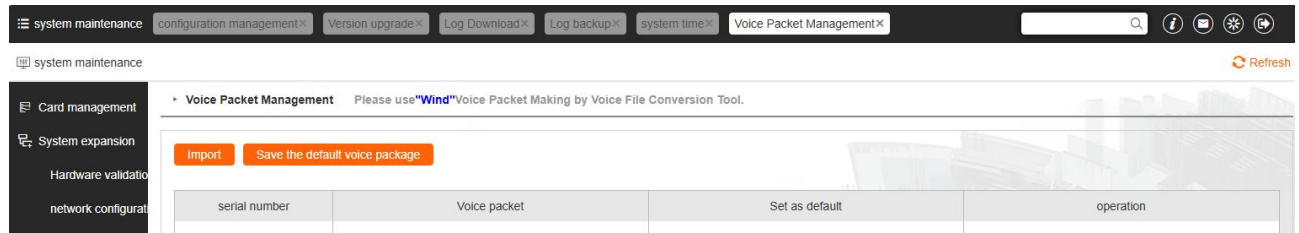
- Step1. Click**System Maintenance>Language Pack Management**to enter the configuration interface.
- Step2. Click**Import**to import a pre-made voice pack.

To create voice packs, you need to use the wind voice file conversion tool

developed by New Rock, please refer to the specific method. [Guidelines for the use of the Windsound Voice File Conversion Tool](#) For details, please refer to

Step3. Click the **Set as Default** checkbox and then click **Save Default Voice Pack** to set the system default voice pack.

Figure4-37 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
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.

Filename	Element
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.
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

Filename	Element
	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
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 Diagnostics** and fill in the destination IP address or host name to start the diagnostics. Diagnostics can be viewed in the **Summary Information** box.

Figure4-38 Ping Diagnostic Interface

► Ping diagnosis

Destination IP address or host name: start

Summary Info:

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 to **System 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 OM8000 interface

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

► Data capture

This function is used for fault analysis or problem location. The connection schematic is as follows.:



● 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. OM8000 Interface Enables Packet Grabbing
3. The PC opens packet capture software (e.g. Wireshark) to capture packets

► Data capture

This function is used for fault analysis or problem location. The connection schematic is as follows.:



Note:

1. Select the mirror port for packet capture (AUX #2 recommended)
2. Connect PC to the mirror port
3. You must connect to the current active chassis for capture. Swap your capture link to the other chassis when switch-over occurs and the other one becomes active
4. The packets between IF cards in the same chassis can not be captured
5. The packets between IF cards across different chassis can be captured
6. Packets in and out of the WAN/AUX ports of the other chassis could not be captured

Open mirroring

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 **SystemMaintenance>SystemTools>License Management**(the menu is pulled to the bottom) and import the License file.

» Authorization import

Authorization File Import: browse import

» Authorization management

Device information

Chassis #1 MAC:

Authorization information

IP Extension Permission Number:	Due date: permanent
SIP Outline Permission Number:	Due date: permanent
API Interface Licensing:	Due date: permanent
PMS Interface License:	Due date: permanent
Dual Hot Standby Permit:	Due date: permanent
Flow Balance Permission:	Due date: permanent
CDR Interface License:	Due date: permanent
Geo-redundant license:	Due date: permanent

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.
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.

Item	Description
CDR interface license	Activation: CDR interface allowed Not activated: CDR interface not allowed

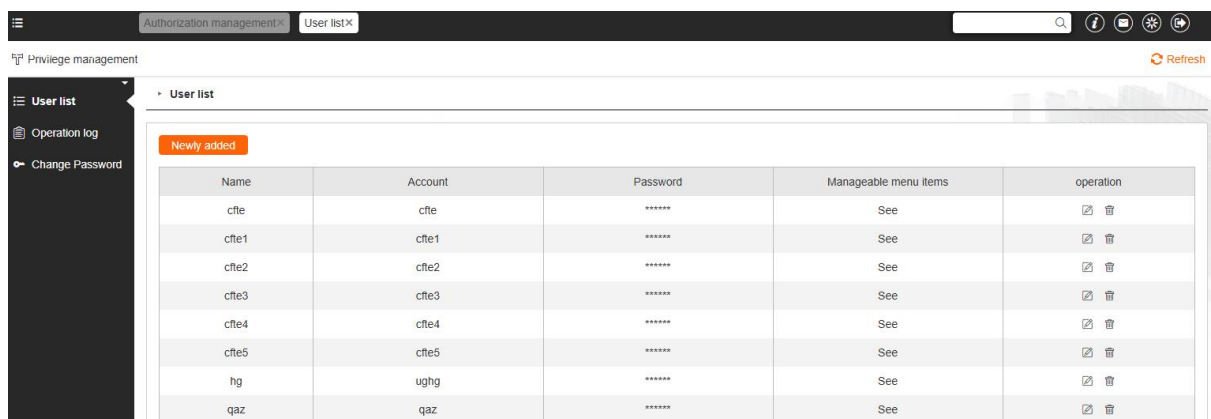
4.9 Rights Management

4.9.1 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. Click **Save**.

• User editor

* Admin account : cfe * Name : cfe * Admin password : * Confirm password :

• Configure Administrator Menu Permissions

configuration note

1.Unchecked means Unavailable
2.Checked means Read only
2.Checked + click edit button means Read-write

☒ Condition monitoring

☒ Device status ☒ Extension state ☒ Outside state ☒ system state

☒ Basic setup

☒ network configuration ☒ Outgoing rule ☒ Switchboard ☒ IVR ☒ Voice management

☒ Caller Answering Group

☐ Extension settings

☒ IP extension ☒ Number filtering ☒ department ☒ Call Number Binding Table

☐ Outside settings

☒ SIP external line ☒ DOD

☒ application service

☒ media ☒ API ☒ Sound recording ☒ Call limit ☒ secretary

☒ Duty table

☒ advanced setting

☒ system ☒ Network management ☒ certificate ☒ Function code ☒ Routing table

☒ Dial detection ☒ SIP compatibility

☒ Safety Center

☒ Security configuration ☒ Visit White List ☒ Violence-proof cracking accounts ☒ Static defense ☒ encryption

☒ system maintenance

☒ Card management ☒ System expansion ☒ alarm management ☒ Log management ☒ System tools

☒ Version upgrade ☒ configuration management

☒ Networking mode

☒ Networking mode

Preservation

4.9.2 Operating Log

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

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

操作日志

名称:

账号:

时间段:

查询

导出

账号	名称	操作内容	操作时间
admin	admin	(1380)LOGIN_ACC_2 to test2[test2]"000011111010000100000001000000	19/09/27 17:20:19
admin	admin	(1380)LOGIN_ACC_1 to test[test]"00002000001000010000000000000000	19/09/27 14:59:15

4.9.3 Modify A Password

Modify administrator password: Go to**Permission Management>Modify Password**, modify it and click**Save**.

Authorization managementUser listChange Password

Privilege management

User list

Operation log

Change Password

Change Password

Old password:

New password:

Confirm the new password:

Preservation

login timeout

overtime: 600

Second (range: 60-7200)

Preservation

Change the general admin password: Go to **Permission Management>User List** and click  to change the password. Click**Save**.

新增

名称	账号	密码	可管理菜单项	操作
hwang	hwang	*****	查看	 管理
test	test	*****	查看	 管理

4.10 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.

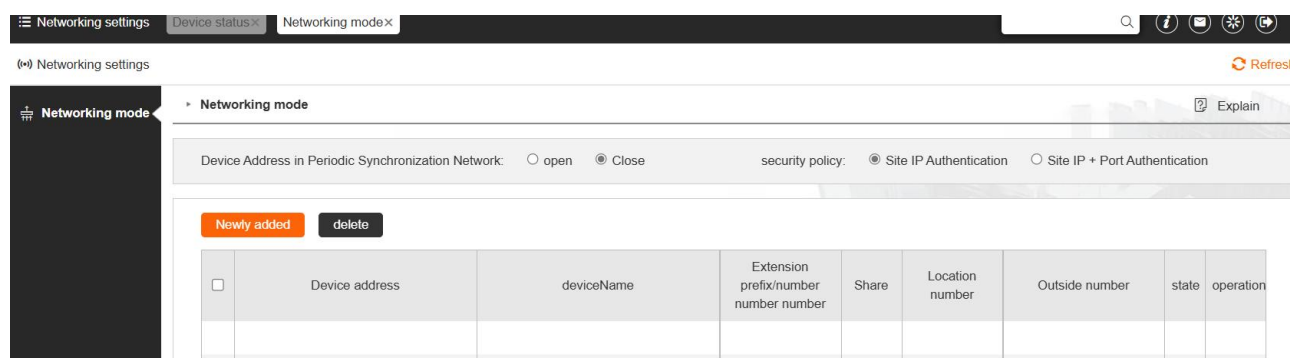
Deployment requires uniform planning of the extension numbers of all devices in the network to avoid number conflicts.

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 to **Networking Settings>Networking Methods**.

Figure4-39 network interface



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

Figure4-40 Network Configuration Interface

Networking mode

Device Address in Periodic Synchronization Network:

☐ open ☒ Close

security policy:

☒ Site IP Authentication ☐ Site IP + Port Authentication

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

Click **New** and enter the management site information.

Figure4-41 Add Site Screen

[illegible]

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.
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 **Add** and 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 **Add** and 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

After **saving** the 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.

5 Common Problems

5.1 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.