Redstone Systems, Inc.

REX Series IP Telephony System

Administrator Manual

REX20

REX50

REX200

REX200-A

REX500

REX1000

Document Version: 12

Release Date: 2025-03-05

Amendment Records

Document Rev. 12（December,2025）

Updated based on REX20，REX50，REX200，REX200-A,REX500,REX1000 Series Rev 2.1.5.241.

Copyright © 2025 Redstone 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 is applicable to REX20，REX50，REX200，REX200-A,REX500,REX1000 Series Rev 2.1.5.241.

The manual guides administrators in setting REX parameters on Web GUI interfaces. Some parameters can be set by using a telephone.

 Copyright © Redstone Systems, Inc

New Features

Number	Introduction of new features in the version
1	One Number, Ten Devices feature, which allows one phone number (i.e., number one) to be registered and bound to up to ten devices at the same time, enhancing the flexibility of numbers and interconnectivity of devices. (Currently support REX500)
2	Room status management function, which is designed for hotel industry. By dialing the specified function code through the extension, the system will push the room status information to the hotel PMS system through messages to realize real-time information update.
3	On the [Application Services > Alarm Notification] screen, the phone alarm function is added. Allows the user to automatically call a specified phone number to alert the user when a specific alarm occurs on the device.
4	Dual power supply status page display function, users can monitor the dual power supply status of the device in real time through the status bar. (Currently support REX1000)
5	The SIP trunk proxy server adds the master and backup function on the basis of the original master and backup mechanism, and terminals are prioritized to be switched between the dual master proxy servers, and are switched to the backup proxy server only when both masters fail.

Copyright © Redstone Systems, Inc

Contents

Amendment Records I
Manual Description II
New Features III
1 Overview 1
1.1 Products 1
1.2 Equipment Structure 2
1.2.1 REX20 2
1.2.2 REX50 5
1.2.3 REX200/REX200-A 8
1.2.4 REX500 12
1.2.5 REX1000 17
1.3 Access to Equipment 19
1.3.1 Connected device 19
1.3.2 Login Device 19
1.4 Introduction to Web Management Interface Layout 22
1.5 Network Configuration 23
1.5.1 Network Parameters (REX20/REX50) 23
1.5.2 Network Parameters (REX200/REX200-A/REX500) 26
1.5.3 Network Parameters (REX1000) 28
1.5.4 Domain name resolution 29
1.5.5 STUN 31
1.5.6 Remote access 34
1.5.7 VPN (REX20/REX50) 38
2 Features 39
2.1 Auto Attendant 39
2.1.1 Configuring the Auto Attendant 39
2.1.2 Customizing and replacing voice files 41
2.1.3 Creating multi-level IVR 45
2.2 Operators/Receptionists 50
2.3 Trunk 53
2.3.1 Analog Trunk (REX1000 does not have an analog external line) 53
2.3.2 SIP Trunk 56
2.3.3 Backup SIP Server Configuration 64
2.3.4 IMS 66

 Copyright © Redstone Systems, Inc

2.3.5 Directly Connected Trunk Groups 68
2.3.6 DID/DOD (REX1000) 70
2.4 Extension 71
2.4.1 Analog Extension (REX1000 does not have analog extensions) 71
2.4.2 IP extension 75
2.4.3 IP extension address authentication 77
2.4.4 One Number Supports Ten Devices 78
2.5 Extension Functions 79
2.5.1 Basic Functions 79
2.5.2 Dialing an outside line 84
2.5.3 Inbound/outbound number filtering 86
2.5.4 Call answering team 87
2.5.5 Extension Status Subscription (REX20/REX50/REX1000) 89
2.5.6 Group Substitution 91
2.5.7 Substitute connection 92
2.5.8 Three-way calling 93
2.5.9 Call Parking 93
2.5.10 DID 93
2.5.11 Binding Incoming Call Numbers to an Extension 94
2.5.12 Function Codes 96
2.5.13 TLS Encryption 97
2.6 Recordings and Messages 98
2.6.1 Recordings 98
2.6.2 Messages 103
2.7 Fax 106
2.8 Multi-Device Networking 108
2.8.1 Assign the extension numbers globally 108
2.8.2 Repeatable extension numbers within the network 112
2.9 System Configuration 119
2.9.1 Built-in storage management 119
2.9.2 Incoming call duty roster 120
2.9.3 Use of color ringtones 122
2.9.4 Background music 123
2.9.5 Uploading Interpolated Voice 124
2.9.6 System time 124
2.9.7 Encryption 126
2.9.8 Routing Tables 128
2.9.9 Dial Detection and Number Bitmap 135
2.9.10 Call Progress Tone 137
2.9.11 SIP Compatibility 138

2.9.12 DTMF 140
2.9.13 Media 141
2.9.14 Call Records 142
2.9.15 API 143
2.9.16 Site attribution area digits 145
2.9.17 SIP Transmission Method 146
2.9.18 Automated Management 146
2.9.19 TR069 148
2.9.20 Ping Diagnostics (REX20/REX50) 149
2.9.21 Voice package management 149
2.9.22 Dual hot standby (REX1000) 153
2.9.23 Remote Support 156
2.9.24 Paging Rules 156
2.9.25 NewLync Service 157
2.9.26 Networking Server 157
2.9.27 Alarm Notification 158
2.10 Security Management 160
2.10.1Firewall 160
2.10.2 Anti-brute-force account break-in 162
2.10.3 Dynamic Defense 164
2.10.4 Call restriction 166
2.10.5 Change Password 167
2.10.6 SSH 168
2.10.7 Ping 169
2.10.8 Web Management 170
2.10.9 Voice security 171
2.10.10 Black/White List 172
2.11 System Maintenance 174
2.11.1 Upgrading 174
2.11.2 Configuration Maintenance 175
2.11.3 Reboot 177
2.11.4 Port Signal Capture (Not supported by REX1000) 177
2.11.5 Ethereal capture 178
2.11.6 Log management 179
2.11.7 Operational Information 180
2.11.8 Dual-System Switching Method 182
2.12 Equipment Maintenance Information 183
2.12.1 Operational status 183
2.12.2 Alarms 183
2.12.3 Product Information 184
2.12.4 Call Messages 185

2.13 Supporting Application Software 186
3 Common Problems 187
3.1 No number display for incoming calls 187
3.2 IP outbound registration issues 188
3.3 IP network connectivity issues 189
3.4 Analog extension not ringing 189
3.5 Wrong date displayed on the phone's caller ID 190
3.6 Extension Volume Small 191
3.7 Analog extension crosstalk 191
3.8 Availability of the R key on analog extensions 191
3.9 Forgetting to customize whitelist results in not being able to log in to the device 192
3.10 Analog Outbound Inbound and Outbound Abnormalities 192
4 OpenVPN Certificate Creation(REX20/REX50) 193
Appendix A IP Extension Registration to Devices 195
Appendix B RJ45 and RJ11 Line Correspondence Table 197

Contents of Figures

Figure 1-1 REX20 Front Panel 2
Figure 1-2 REX20 Rear Panel 3
Figure 1-3 RJ45 -RS232 Serial Connection Cable 4
Figure 1-4 USB-RS232 Serial Connection Cable 4
Figure 1-5 REX50 Front Panel 5
Figure 1-6 REX50 Rear Panel 7
Figure 1-7 REX200/REX200-A Front Panel 8
Figure 1-8 REX200/REX200-A Rear Panel - Single AC Power Module 10
Figure 1-9 REX200/REX200-A Rear Panel - Single Direct AC Power Module 10
Figure 1-10 User line port schematic 13
Figure 1-11 RJ45 Receptacle Port Pinout Specification Table 13
Figure 1-12 REX500 front panel 14
Figure 1-13 REX500 Rear Panel - Single AC Power Module 15
Figure 1-14 REX500 Rear Panel - Single DC Power Module 15
Figure 1-15 REX1000 Front Panel 17
Figure 1-16 REX1000 rear panel 18
Figure 1-17 Installation wiring diagram 19
Figure 1-18 Login screen 21
Figure 1-19 Prompt to change the administrator login password screen 22
Figure 1-20 Web Management Interface 22
Figure 1-21 Network Configuration Interface 24
Figure 1-22 ETH2 Configuration Interface 26
Figure 1-23 AUX&EXP configuration interface 28
Figure 1-24 DNS Server Configuration Interface 30
Figure 1-25 STUN Configuration Interface 31
Figure 1-26 Network management interface 32
Figure 1-27 4G NAT operations options screen 33
Figure 1-28 802.1X Configuration Interface 34
Figure 1-29 P2P traversal Configuration Interface 35
Figure 1-30 Remote Access Configuration Interface 36
Figure 1-31 Router Port Mapping Configuration Interface 37
Figure 1-32 VPN Configuration Interface 38
Figure 2-1 Auto Attendant Configuration Screen 39
Figure 2-2 Text-to-welcome message interface 42

 Copyright © Redstone Systems, Inc

Figure 2-3 Text-to-welcome message interface (after installing Wind Sound) 42
Figure 2-4 Voice file management interface 43
Figure 2-5 Upload Welcome Message Screen 43
Figure 2-6 Upload welcome message screen (after installing Wind Sound) 44
Figure 2-7 IVR Flowchart 46
Figure 2-8 IVR Configuration Interface 46
Figure 2-9 IVR1 Configuration Interface 47
Figure 2-10 IVR2-1 Configuration Interface 49
Figure 2-11 IVR2-2 Configuration Interface 50
Figure 2-12 Operator Configuration Screen 51
Figure 2-13 Analog trunk Configuration Interface 1 53
Figure 2-14 Analog Outside Line Advanced Settings screen 55
Figure 2-15 SIP Outbound Configuration Interface 57
Figure 2-16 SIP Outbound Configuration Interface 61
Figure 2-17 SIP Outbound Registration Options Screen 62
Figure 2-18 Backup Server Configuration Interface 65
Figure 2-19 IMS Configuration Interface 67
Figure 2-20 Register for the multi-platform configuration screen 68
Figure 2-21 Direct Connect Trunk Group Configuration Screen 69
Figure 2-22 Linear (DID/DOD) Configuration Screen 70
Figure 2-23 Analog Extension Configuration Interface 71
Figure 2-24 Analog Extension Advanced Settings Screen 74
Figure 2-25 IP Extension Account Configuration Screen 76
Figure 2-26 IP Authentication Configuration Interface 77
Figure 2-27 One Number Supports Ten Devices Setting Interface 78
Figure 2-28 Extension Function Configuration Interface 79
Figure 2-29 Outbound Rule Configuration Interface 84
Figure 2-30 Number Filtering Configuration Interface 86
Figure 2-31 Call Answer Group Configuration Interface 87
Figure 2-32 Extension Status Subscription Screen 89
Figure 2-33 Selecting an Extension Model 90
Figure 2-34 Subscription Extension 90
Figure 2-35 Extension Status Subscription Main Screen 91
Figure 2-36 Department Configuration Screen 92
Figure 2-37 Extension Department Selection Screen 92
Figure 2-38 Linear (DID) Configuration Screen 94
Figure 2-39 Call Binding Number Table Interface 94
Figure 2-40 Function Code Configuration Interface 96
Figure 2-41 IP Extension Setting Interface 97

Figure 2-42 TLS Settings Screen 97
Figure 2-43 Remote Storage Configuration Interface 98
Figure 2-44 Extension Recording Configuration Interface1 99
Figure 2-45 Remote Recording/Local Message Configuration Interface 100
Figure 2-46 Extension Recording Configuration Screen 2 100
Figure 2-47 Built-in Storage Configuration Interface 101
Figure 2-48 Extension Recording Configuration Interface3 102
Figure 2-49 Message Configuration Interface 104
Figure 2-50 Fax Mode Configuration Interface (REX20/REX50) 106
Figure 2-51 Fax Mode Configuration Interface (REX200/REX200-A/REX500/REX1000) 106
Figure 2-52 Networking Solution Selection Interface 109
Figure 2-53 Network Configuration Interface 109
Figure 2-54 Add Site Interface 110
Figure 2-55 Management Site Local Domain Name Configuration Interface 113
Figure 2-56 Management Site Network Configuration Interface 1 113
Figure 2-57 Select Device Networking Role Interface 114
Figure 2-58 Management Site Configuration Interface 2 114
Figure 2-59 Management Site Network Configuration Interface 3 114
Figure 2-60 Management Site Network Configuration Interface 4 116
Figure 2-61 Management Site Network Configuration Interface 5 116
Figure 2-62 Common Site Local Domain Configuration Interface 117
Figure 2-63 Common Site Networking Configuration Interface 1 117
Figure 2-64 Common Site Networking Configuration Interface 2 118
Figure 2-65 Common Site Networking Configuration Interface 3 118
Figure 2-66 Common Site Networking Configuration Interface 4 118
Figure 2-67 Built-in Storage Management Interface 120
Figure 2-68 Duty List Screen 120
Figure 2-69 Automated Attendant Interface 122
Figure 2-70 Color Ringtone File Upload Configuration Interface 122
Figure 2-71 Background Music Configuration Interface 124
Figure 2-72 System Time Configuration Interface 125
Figure 2-73 Encryption Interface 126
Figure 2-74 Routing Table Configuration Interface of Number Transformation 128
Figure 2-75 Routing Table Configuration Interface of Call Duration Restriction 131
Figure 2-76 Dialing Rule Configuration Screen 135
Figure 2-77 Tone Setting Interface 137
Figure 2-78 SIP Compatibility Interface 138
Figure 2-79 DTMF Interface 140
Figure 2-80 Media Configuration Interface 141

 Copyright © Redstone Systems, Inc

Figure 2-81 Call Log Configuration Screen 143
Figure 2-82 API Configuration Interface 144
Figure 2-83 Attribution Area Bit Number Configuration Screen 145
Figure 2-84 SIP Transmission Mode Configuration Interface 146
Figure 2-85 Automatic Management Configuration Interface 147
Figure 2-86 TR069 Configuration Interface 148
Figure 2-87 Ping Diagnostic Interface 149
Figure 2-88 Voice Pack Configuration Interface 150
Figure 2-89 Voice Pack Configuration Interface 150
Figure 2-90 Dual Machine Hot Standby Interface 154
Figure 2-91 Remote Support Interface 156
Figure 2-92 Broadcast Rule Setting Screen 156
Figure 2-93 NewLync Service Settings screen 157
Figure 2-94 Networking Server Settings Screen 157
Figure 2-95 Alarm Notification Interface 158
Figure 2-96 Static Defense Configuration Interface 161
Figure 2-97 Anti-Violence Breach Account (Login Retry Lockout) Configuration Screen 163
Figure 2-98 Anti-Violence Breach prevention (Lock List) Screen 163
Figure 2-99 Dynamic Defense Configuration Interface 164
Figure 2-100 This defense list is deleted after the device reboots. Dynamic Defense (Defense List) Interface 165
Figure 2-101Call Barring Configuration Screen 167
Figure 2-102 Change Password Interface 167
Figure 2-103 SSH Configuration Interface 168
Figure 2-104 Ping Configuration Interface 169
Figure 2-105 Web Management Configuration Interface 170
Figure 2-106 Voice Security Configuration Interface 171
Figure 2-107 Call Black/White List Configuration Screen 172
Figure 2-108 Extension Black/White List Configuration Interface 173
Figure 2-109 Software Upgrade Interface 174
Figure 2-110 Secondary Upgrade Page 175
Figure 2-111 Configuration Import Screen 176
Figure 2-112 Configuration Export Screen 176
Figure 2-113 Restore Factory Configuration Interface 176
Figure 2-114 Functional License Configuration Screen 176
Figure 2-115 Reboot Screen 177
Figure 2-116 Port Capture Interface 178
Figure 2-117 Data Capture Interface 179
Figure 2-118 Log Download Interface 179

Figure 2-119 Operation Information Screen 181
Figure 2-120 Running Status Interface 183
Figure 2-121 Alarm Interface 184
Figure 2-122 Product Information Screen 185
Figure 2-123 Call Message Screen 185
Figure 4-1 IP Phone Registration Screen 195
Figure 4-2 RJ45 user cable connection diagram 197

 Copyright © Redstone Systems, Inc

Contents of Tables

Table 1-1 REX20 Product Model 2
Table 1-2 REX20 Indicator Status Description 2
Table 1-3 REX20 Interface Description 4
Table 1-4 REX50 Product Model 5
Table 1-5 REX50 Indicator Status Description 5
Table 1-6 REX50 Interface Description 7
Table 1-7 REX200/REX200-A Model No. 8
Table 1-8 REX200/REX200-A Indicator Meaning Table 9
Table 1-9 REX200/REX200-A System Operation Status Display Comparison Table 10
Table 1-10 REX200/REX200-A Interface Description 11
Table 1-11 REX500 Model No. 12
Table 1-12 REX500 interface card 12
Table 1-13 REX500 Indicator Meaning Table 14
Table 1-14 REX500 System Operation Status Display Comparison Table 15
Table 1-15 REX500 Interface Description 16
Table 1-16 REX1000 Model No. 17
Table 1-17 REX1000 Indicator Meaning Table 17
Table 1-18 REX1000 Interface Description 18
Table 1-19 Login Interface Parameters 21
Table 1-20 Web Interface Layout Description 23
Table 1-21 Description of network parameters 24
Table 1-22 ETH2 Parameter Description 27
Table 1-23 AUX&EXP Parameter Description 29
Table 1-24 DNS Server Parameter Description 30
Table 1-25 Description of STUN interface parameters 31
Table 1-26 Functional definition of the 4G NAT operations button 33
Table 1-27 802.1X Interface Parameter Description 34
Table 1-28 Description of penetration parameters 36
Table 1-29 Description of extranet access parameters 37
Table 1-30 Port mapping parameter 37
Table 1-31 VPN Parameter Description 38
Table 2-1 Automated Operator Parameters 40
Table 2-2 The device has two voices by factory default 41

 Copyright © Redstone Systems, Inc

Table 2-3 Microphone Recording Welcome Note 44
Table 2-4 IVR Configuration Interface Parameters 47
Table 2-5 IVR Menu Event Configuration Interface Parameters 48
Table 2-6 Operator Parameters 51
Table 2-7 Analog Outside Line Configuration Parameters 53
Table 2-8 Advanced configuration parameters for the proposed external line 55
Table 2-9 Description of SIP outbound registration parameters 57
Table 2-10 SIP Outbound Interface Parameter Description 61
Table 2-11 Parameter Description of SIP Outbound Registration Options 63
Table 2-12 Description of Backup Server Configuration Parameters 65
Table 2-13 Description of IMS interface parameters 67
Table 2-14 Parameter description of the directly connected trunk group 69
Table 2-15 Linear (DID/DOD) Parameter Description 70
Table 2-16 Analog Extension Configuration Parameters Description 72
Table 2-17 Analog Extension Advanced Setup Parameter Description 74
Table 2-18 IP Extension Configuration Parameter Description 76
Table 2-19 Extension Basic Functions 79
Table 2-20 Outbound call rule parameter description 84
Table 2-21 Parameter Description of Number Filtering Interface 87
Table 2-22 Parameter description of the call answering group 88
Table 2-23 Extension Subscription Indicator Status Description Table 89
Table 2-24 Parameter Description of Caller Binding Number Form 95
Table 2-25 Managing audio files 102
Table 2-26 Parameter description of voice message sending server 105
Table 2-27 Manage Message Files 105
Table 2-28 Fax Interface Parameter Description 107
Table 2-29 Security Policy Parameters 110
Table 2-30 Site Add Interface Parameters 111
Table 2-31 Description of the parameters of the network planning interface 115
Table 2-32 Networking Dialing Prefix Interface Parameter Description 116
Table 2-33 Description of Outgoing Resource Interface Parameters 116
Table 2-34 Description of duty roster parameters 121
Table 2-35 Description of system time parameters 125
Table 2-36 Description of encryption parameters 126
Table 2-37 Explanation of the rules of the common numbered digit map 136
Table 2-38 Description of Beep Parameters 137
Table 2-39 Examples of customized tone rules 138
Table 2-40 SIP Compatibility Parameter Description 138
Table 2-41 DTMF Parameter Description 140

Table 2-42 Description of media parameters 142
Table 2-43 API Interface Parameter Description 144
Table 2-44 Explanation of attributed area code parameters..... 145
Table 2-45 SIP transmission method parameter description 146
Table 2-46 Automatic management of parameters..... 147
Table 2-47 TR069 Parameter Description..... 148
Table 2-48 System voice prompt file..... 150
Table 2-49 Parameter description of the master-standby switchover 155
Table 2-50 Alarm Notification Parameter Description..... 158
Table 2-51 Description of alarm notification options..... 159
Table 2-52 Description of whitelisting parameters..... 160
Table 2-53 Static defense parameters 161
Table 2-54 Anti-brute-force account break-in (login retry lockout) parameters 163
Table 2-55 Anti-brute-force account (lockout list) display information..... 163
Table 2-56 Dynamic Defense (Rule Configuration) Parameters 165
Table 2-57 Dynamic Defense (Defense List) Display Information 165
Table 2-58 (Subsequent selection of (batch) mobile defense lists to static defense lists..... 166
Table 2-59 Web Management Interface Parameter Description..... 170
Table 2-60 Description of voice security interface parameters..... 171
Table 2-61 Restarting the Configuration Interface 177
Table 2-62 Log Download Interface Parameter Description 180
Table 2-63 Operational Information Interface Parameters..... 181
Table 2-64 Classification of alarm messages..... 184
Table 2-65 List of applications..... 186
Table 3-1 Solution to SIP Outbound Registration Problems..... 188
Table 3-2 Extension call volume is low solution..... 191
Table 4-1 IP Phone Registration Parameters 196
Table 4-2 RJ45 Socket Pin Leader Specification..... 197

 Copyright © Redstone Systems, Inc

1 Overview

1.1 Products

REX series IPPBX products are multifunctional business office telephone systems for branch offices of small and medium-sized enterprises. This series of products integrates the functions of VoIP, voice, fax, and recording, and is compatible with a variety of business platforms and terminals such as CallManager, Broadsoft, Skype for business, Huawei IMS, and Asterisk, providing a diverse range of converged communication solutions.

Supports local and remote management via Web GUI or SSH, automatic management (Auto provisioning), centralized management of TR069/TR104/TR106. Supports remote management and monitoring of equipment through the Redstone cloud service.

In addition, NewLync digital collaboration platform and NeeHau business assistant software developed by Redstone can be used together to support intelligent communication functions such as cell phone extension, instant multi-party conference, call records, address book click dialing, customer information management, etc, which help enterprises communicate efficiently among switchboards, employees and customers and lay a solid foundation for enterprises to analyze the data of their core business.

 Copyright © Redstone Systems, Inc

1.2 Equipment Structure

1.2.1 REX20

Table 1-1 REX20 Product Model

Model number	Number of Interface Cards	Number of analog external interfaces	Number of analog extension interfaces
REX20-4S	1	0	4
REX20-4FXO	1	4	0
REX20-2S/2	1	2	2

Figure 1-1 REX20 Front Panel



Table 1-2 REX20 Indicator Status Description

Indicator light	Blinker status	Explanation
PWR (green)	Blinking green	Device startup in progress.
	Steady green	Startup complete.
	Off	Failure to power up or power failure.
STU (red, green)	Steady red	The WAN port does not get the IP address, such as the WAN port is not connected to the network cable, DHCP to get the WAN port address failure, IP address conflict, PPPoE dialing failure, etc.
	Blinking red	Device startup or Kupdate upgrade in progress.
	Steady green	WAN port gets the address, SIP external line registers successfully.
	Alternately flashing red and green	WAN port gets address, SIP outbound registration fails.
	Blinking green	WAN port gets address, no registration on SIP outside line.
USB (green)	Steady green	Correctly identifying storage devices connected to the USB port.
	Blinking green	3G/4G Internet card dialing success*
	Off	Unconnected USB device, 3G/4G Internet card dialing

 Copyright © Redstone Systems, Inc

Indicator light	Blinker status	Explanation
		failure or no dialing*
WAN (green)	Steady green	WAN connection established, but no service flow.
	Blinking green	WAN connection established with business flow.
	Off	WAN port not wired.
PC (green)	Steady green	Link is connected but no service flow.
	Blinking green	With business flow transmission.
	Off	The link is not connected.
VOICE (green-FXS, yellow-FXO)	Displays the line type status:	
	Blinking yellow	The line is detected as an outside line (FXO) during device startup.
	Blinking green	The line is detected as an extension line (FXS) during device startup.
	Off	No line detected (e.g., unplugged line card, damaged port, etc.)
	Work Status:	
	Steady yellow	Inbound or outbound via analog outside line.
	Blinking yellow	Analog outside caller ringing.
	Steady green	Analog extension off-hook or on-hook.
	Blinking green	Analog extension ringing.
	Off	Idle state.
	Note: During the startup process of the device, there are about 30 seconds of line type display status, and the startup is completed to return to the normal working state.	
Button Description:	RST	Restore the factory default settings of the device. Press this button with a pointed object for 3~5 seconds until the STU indicator is flashing red, then release it and wait for the device reboot to complete

Figure 1-2 REX20 Rear Panel



 Copyright © Redstone Systems, Inc

Table 1-3 REX20 Interface Description

Connector	Definition
FXS	Analog extension interface (RJ11) for connecting analog phones, fax machines, POS machines.
FXO	Analog outside line interface (RJ11) for connection to the public switched telephone network (PSTN).
PC/WAN	The PC port is used to connect to a computer. The WAN port is used to connect to the uplink network. Two 100 Gigabit Ethernet switching ports (RJ45) that share a common IP address. The IP address is obtained by DHCP by default, and the default address 192.168.2.218 is used when the acquisition fails. The address can be modified in Basic Configuration>Network. Note: The REX does not automatically assign an address to the computer, you must manually configure the computer's IP address to be on the same network segment as the REX.
USB	USB port for connecting a USB storage device. Note: The device contains another 16GB of internal storage.
CON	Serial port for connecting a serial terminal for background debugging. Note: Not normally used. A dedicated RJ45-RS232 serial connection cable is required to connect to the RS232 port on the PC. This connection cable needs to be made or purchased. If connecting to a laptop that does not have an RS232 port, a USB to RS232 serial connection cable is also required.
RST	Reset button for restoring factory settings.
PWR	Power connector for connection to a power source. Note: Use the power adapter provided with the unit.
Grounding terminal	Used to connect the ground wire.

Figure 1-3 RJ45 -RS232 Serial Connection Cable



Figure 1-4 USB-RS232 Serial Connection Cable



 Copyright © Redstone Systems, Inc

1.2.2 REX50

Table 1-4 REX50 Product Model

Model number	Interface Card Name	Number of Interface Cards	Number of analog external interfaces	Number of analog extension interfaces
REX50-12S	401A-4S	3	0	12
REX50-10S/2	401A-2S/2	1	2	10
	401A-4S	2		
REX50-8S/4	401A-2S/2	2	4	8
	401A-4S	1		
REX50-6S/6	401A-2S/2	3	6	6

Figure 1-5 REX50 Front Panel



Table 1-5 REX50 Indicator Status Description

Indicator light	Blinker status	Particular
PWR (green)	Blinking green	Device startup in progress.
	Steady green	Startup complete.
	Off	No power up or power failure.
STU (red, green)	Steady red	The WAN port does not get the IP address, such as the WAN port is not connected to the network cable, DHCP to get the WAN port address failure, IP address conflict, PPPoE dialing failure, etc.
	Blinking red	Device startup or Kupdate upgrade in progress.
	Steady green	WAN port gets the address, SIP external line registers successfully.
	Alternately flashing red and green	WAN port gets address, SIP outbound registration fails.
	Blinking green	WAN port gets address, no registration on SIP outside line.
USB (green)	Steady green	Correctly identifying storage devices connected to the USB port.
	Blinking green	3G/4G Internet card dialing success*
	Off	Unconnected USB device, 3G/4G Internet card dialing (not supported

Indicator light	Blinker status	Particular
		at this time) failed or not dialing.
WAN (green)	Steady green	WAN connection established, but no service flow.
	Blinking green	WAN connection established with business flow.
	Off	WAN interface not wired.
PC (green)	Steady green	Link is connected but no service flow.
	Blinking green	With business flow transmission.
	Off	The link is not connected.
VOICE (green-FXS, yellow-FXO)	Displays the line type status:	
	Blinking yellow	The line is detected as an outside line (FXO) during device startup.
	Blinking green	The line is detected as an extension line (FXS) during device startup.
	Off	No line detected (e.g., unplugged line card, damaged port, etc.)
	Work status:	
	Yellow long bright	Inbound or outbound via analog outside line.
	Blinking yellow	Analog outside caller ringing.
	Steady green	Analog extension off-hook or on-hook.
	Blinking green	Analog extension ringing.
	Off	Idle state.
	Note: During the startup process of the device, there are about 30 seconds of line type display status, and the startup is completed to return to the normal working state.	
Button Description		
RST	Restore the factory default settings of the device. Press this button with a pointed object for 3~5 seconds until the STU indicator is flashing red, then release it and wait for the device reboot to complete.	

*This model does not support 3G/4G internet card dial-up internet access for the time being.

 Copyright © Redstone Systems, Inc

Figure 1-6 REX50 Rear Panel



Table 1-6 REX50 Interface Description

Connector	Definition
FXS	Analog extension interface (RJ11) for connecting analog phones, fax machines, POS machines.
FXO	Analog outside line interface (RJ11) for connection to the public switched telephone network (PSTN).
PC/WAN	The PC port is used to connect to a computer. The WAN port is used to connect to the uplink network. Two 100 Gigabit Ethernet switching ports (RJ45) that share a common IP address. The IP address is obtained by DHCP by default, and the default address 192.168.2.218 is used when the acquisition fails. The address can be modified in Basic Configuration>Network. Note: The REX does not automatically assign an address to the computer, you must manually configure the computer's IP address to be on the same network segment as the REX.
USB	USB port for connecting a USB storage device. Note: The device contains another 16GB of internal storage.
CON	Serial port for connecting a serial terminal for background debugging. Note: Not normally used. A dedicated RJ45-RS232 serial connection cable is required to connect to the RS232 port on the PC. This connection cable needs to be made or purchased by yourself. If connecting to a laptop that does not havean RS232 port, a USB to RS232 serial connection cable is also required.
RST	Reset button for restoring factory settings.
PWR	Power connector for connection to a power source. Note: Use the power adapter provided with the unit.
Grounding terminal	Used to connect the ground wire.

 Copyright © Redstone Systems, Inc

1.2.3 REX200/REX200-A

Table 1-7 REX200/REX200-A Model No.

Model number		Number of analog external interfaces	Number of analog extension interfaces
REX200/REX200-A	REX200/REX200-A-8s/8	8	8
	REX200/REX200-A-16s	0	16
	REX200/REX200-A-16fxo	16	0
	REX200/REX200-A-16s/16	16	16
	REX200/REX200-A-24S	0	24
	REX200/REX200-A-24s/8	8	24
	REX200/REX200-A-24s/24	24	24
	REX200/REX200-A-32s	0	32
	REX200/REX200-A-32fxo	32	0
	REX200/REX200-A-32s/16	16	32
	REX200/REX200-A-40s/8	8	40
	REX200/REX200-A-48s	0	48
	REX200/REX200-A-48fxo	48	0

Figure 1-7 REX200/REX200-A Front Panel



Table 1-8 REX200/REX200-A Indicator Meaning Table

Indicator light	Flashing light status	Particular
PWR (red, green)	Steady green	Power on.
	Off	Power not connected.
	Steady red	Power supply abnormality.
STU (red, green)	Blinking green	Equipment in operation.
	Steady red	Device startup in progress.
	Blinking red	The system software is starting and has not yet finished starting. At this point the system is in diagnostic mode and can be operated on a limited basis.
	Off	System Lock.
ALM (red, green)	Off	No alarm conditions.
	Blinking red	Generation of alarms (alarms indicated by the letters C, E, T of the LED status display matrix)
	Steady red	Generation of alarms (alarms indicated by letter D of the LED status display matrix)
ETH1/ETH2 (left and right sides)	Long green light on the right side	The link is connected.
	Yellow flashing on the left side	With business flow transmission.
	Lights out on both sides	The link is not connected.
LED status display light matrix	Indicates line type or status during device startup (first 10 seconds) or when disconnecting all network port connections:	
	Steady green	The port is detected as an FXS port.
	Blinking green	The port is detected as an FXO port.
	Off	The port is not detected (possible reasons are port corruption, etc.)
	Indicates line call status when the unit is operating normally:	
	Steady green	Inbound or outbound via FXO port. FXS port picker.
	Blinking green	Ringing signal detected on FXO port. FXS port sends a ringing signal.
	Off	Idle state.
Button Description		
RST	Restore the factory default settings of the device. Press this button with a pointed object for more than 3 seconds until both the STU and ALM indicators are green and always on, then release it and wait for the device reboot to complete.	

 Copyright © Redstone Systems, Inc

Table 1-9 REX200/REX200-A System Operation Status Display Comparison Table

Blinking letter	Status sense
C	Device IP address conflicts with IP addresses of other devices on the LAN
D	Device startup failure
E	Network failure
P	Device is in the middle of a system software upgrade (for BIN upgrades or IMG file upgrades only)
T	The application has exited (the device is unusable)

Figure 1-8 REX200/REX200-A Rear Panel - Single AC Power Module



Figure 1-9 REX200/REX200-A Rear Panel - Single Direct AC Power Module



Table 1-10 REX200/REX200-A Interface Description

Connector	Definition
Front panel	
	Corresponds to the 4 x 4 LED status display lamp matrix on the interface board. Each column corresponds to four phone lines on an RJ45, the first column on the left from top to bottom corresponds to lines 1 to 4, the rightmost column from top to bottom corresponds to lines 13 to 16, and so on in the center.
	Each interface board card corresponds to 4 RJ45 sockets, and each RJ45 socket corresponds to 4 pairs of analog telephone lines. Use Category 5 Ethernet cables to connect the interface board to the patch panel when installing the unit, see the pinout specifications for Appendix B for pinout specifications. Note: The number of interface boards will vary between models. The three interface board cards are serial numbered from left to right as plug-in card #1 (line numbers from 1 to 16), plug-in card #2 (line numbers from 17 to 32), and plug-in card #3 (line numbers from 33 to 48).
Rear panel	
RST	Restore the factory default settings of the device. Press this button with a pointed object for more than 3 seconds until both the STU and ALM indicators are green and always on, then release it and wait for the device reboot to complete.
CON	Configuration port for local management and debugging.
USB	USB port.
ETH1/ETH2	Two 100Gb Ethernet switching ports share the same IP address, the default IP address is 192.168.2.240, which can be changed in "Basic Configuration > Network".
	AC power input connector for 100V to 240V alternating current (AC) voltage.
	DC power input connector for inputting -48V direct current (DC) voltage.
	Grounding post.

 Copyright © Redstone Systems, Inc

1.2.4 REX500

Table 1-11 REX500 Model No.

Product Model	Number of analog extension (FXS) ports	Number of analog external (FXO) ports	Parameters
REX500-NA	Determined by the type and number of interface cards purchased		Single exchange device (telecommunications)
REX500-NA -2AC			Dual AC equipment
REX500-NA -1DC			Single DC device
REX500-NA -2DC			Dual DC equipment

Table 1-12 REX500 interface card

Model number	Number of analog extension (FXS) ports	Number of analog external (FXO) ports
24FXS	24	0
24FXO	0	24
16FXS+8FXO	16	8
12FXS+12FXO	12	12

Introduction to voice interface cards (REX500)

Each voice interface card has six RJ45 subscriber line interfaces, each RJ45 interface can be connected to four pairs of telephone lines, the use of Category 5 network cable compression RJ45 crystal head, and the other end of the cable in accordance with the interface number and the order of pairs of wires connected to the lightning-proof distribution frame (PT2400 or PT4800), the wiring mode see: Figure 1-11 RJ45 socket port pinout lead specification table.

Note Do not connect energized lines such as analog trunks (external lines) or PBX extension lines to the FXS port to avoid damage to the FXS port.

 Copyright © Redstone Systems, Inc

Figure 1-10 User line port schematic

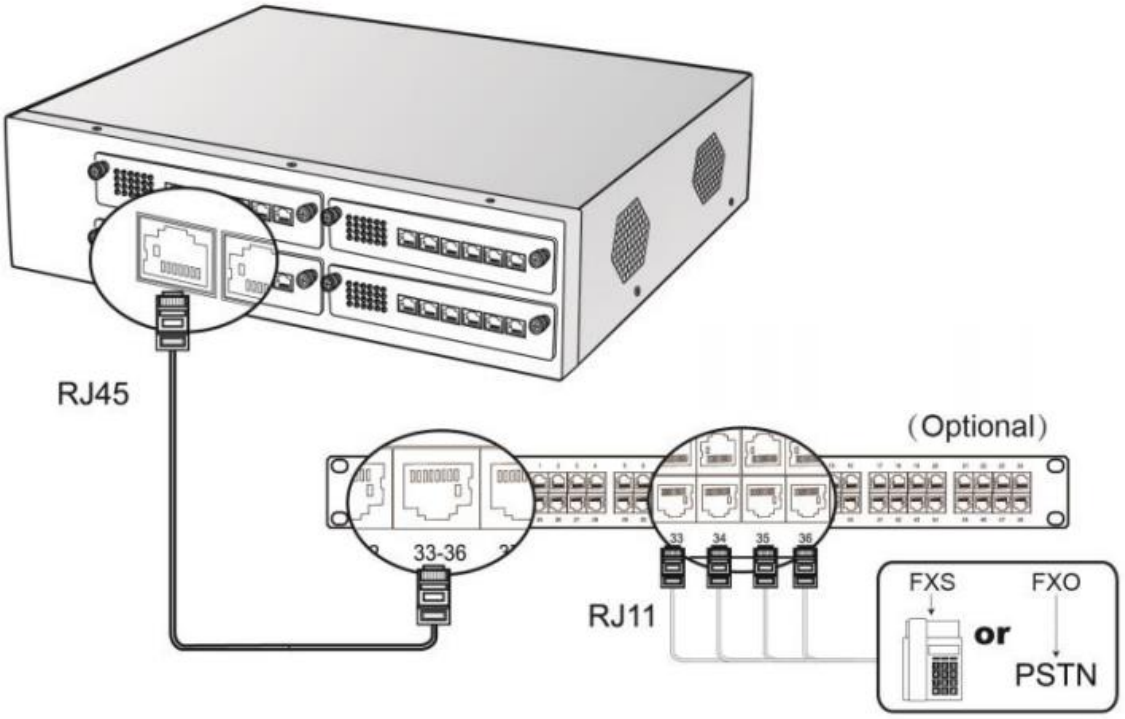


Figure 1-11 RJ45 Receptacle Port Pinout Specification Table

RJ45 Pin Number	1	2	3	4	5	6	7	8
Analog Line Number	1st Pair		2nd Pair (1)	3rd Pair		2nd Pair (2)	4th Pair	
Wire Type	TIP1	RING1	TIP2	TIP3	RING3	RING2	TIP4	RING4

Figure 1-12 REX500 front panel



Table 1-13 REX500 Indicator Meaning Table

Indicator light	Blinker status	Particular
PWR (red, green)	Steady green	Power on
	Off	Power not connected
	Steady red	Power supply abnormality
STU (red, green)	Blinking green	Equipment in operation
	Steady red	Device startup in progress
	Blinking red	The system software is starting and has not yet finished starting. At this point the system is in diagnostic mode and can be operated on a limited basis.
	Off	System Lock
ALM (red, green)	Off	No alarm conditions
	Blinking red	Generation of alarms (alarms indicated by the letters C, E, T of the LED status display matrix)
	Steady red	Generation of alarms (alarms indicated by letter D of the LED status display matrix)
ETH1/ETH2 (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
USB (green)	Steady green	Correctly identifying storage devices connected to the USB port
	Off	Unconnected USB device
LED status display light matrix	Indicates line type or status during device startup (first 10 seconds) or when disconnecting all network port connections:	
	Steady green	The port is detected as an FXS port
	Blinking green	The port is detected as an FXO port
	Off	The port is not detected (possible reasons are port corruption, etc.)
	Indicates line call status when the unit is operating normally:	

 Copyright © Redstone Systems, Inc

	Steady green	Inbound or outbound via FXO port FXS port picker
	Blinking green	Ringing signal detected on FXO port FXS port sends a ringing signal
	Off	Idle state

Table 1-14 REX500 System Operation Status Display Comparison Table

Blinking letter	Status sense
C	Device IP address conflicts with IP addresses of other devices on the LAN
D	Device startup failure
E	Network failure
P	Device is in the middle of a system software upgrade (for BIN upgrades or IMG file upgrades only)
T	The application has exited (the device is unusable)

Figure 1-13 REX500 Rear Panel - Single AC Power Module



Figure 1-14 REX500 Rear Panel - Single DC Power Module

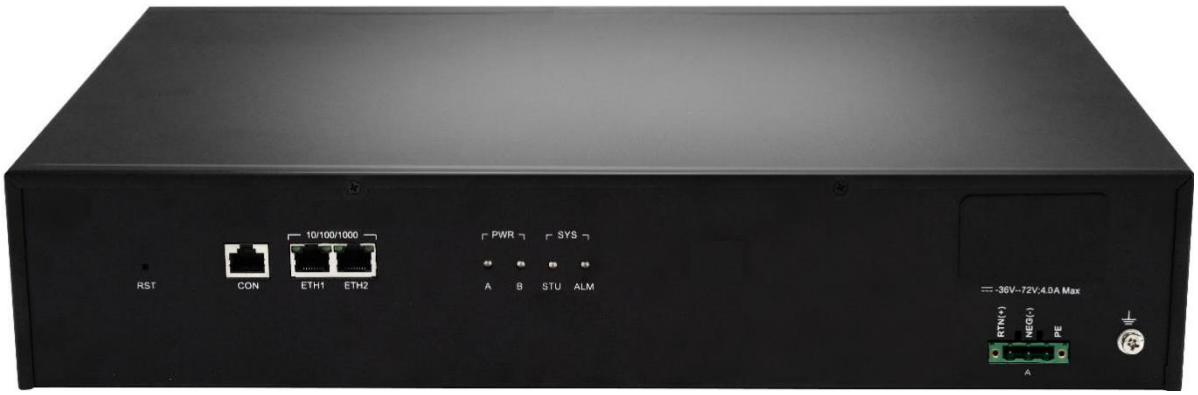


Table 1-15 REX500 Interface Description

Connector	Definition
Front panel	
	A matrix of 4 x 6 (4 rows and 6 columns) LED status display lights on the interface board. Each column corresponds to four phone lines on an RJ45, the first column on the left from top to bottom corresponds to lines 1 to 4, the rightmost column from top to bottom corresponds to lines 21 to 24, and so on in the center.
Slot1~4	Interface slots, each of which can be equipped with an optional interface board card. Each interface board card corresponds to 4 RJ45 sockets, and each RJ45 socket corresponds to 4 pairs of analog telephone lines. Use Category 5 Ethernet cables to connect the interface board to the patch panel when installing the unit, see the pinout specifications for Appendix B for pinout specifications. The four interface boards are arranged in serial numbers from left to right, top to bottom. The upper left plug-in card is plug-in card #1 (analog telephone line numbers from 1 to 24), the upper right plug-in card is plug-in card #2 (line numbers from 25 to 48), the lower left plug-in card is plug-in card #3 (line numbers from 49 to 72), and the lower right plug-in card is plug-in card #4 (line numbers from 73 to 96). Note: Replacing a board with power has no effect on other board applications except for the board being replaced. If the board to be replaced is working properly, simply reboot the unit at the appropriate time.
Rear panel	
Rst	Restore the factory default settings of the device. Press this button with a pointed object for more than 3 seconds until both the STU and ALM indicators are green and always on, then release it and wait for the device reboot to complete.
Con	The configuration port (CON) is used for local management and debugging.
Eth1/eth2	Two Gigabit Ethernet switching ports share the same IP address, the default IP address is 192.168.2.240, which can be changed in "Basic Configuration > Network".
	AC power input connector for 100V to 240V alternating current (AC) voltage.
	DC power input connector for inputting -48V direct current (DC) voltage.
	Grounding post.

 Copyright © Redstone Systems, Inc

1.2.5 REX1000

Table 1-16 REX1000 Model No.

Product Model	Number of analog extension (FXS) ports	Number of analog external (FXO) ports	Definition
REX1000	0	0	1 model only and only supports single AC power supply

Figure 1-15 REX1000 Front Panel



Table 1-17 REX1000 Indicator Meaning Table

Indicator light	Flashing light status	Particular
PWR (green)	Steady green	Power on.
	Off	Power not connected
STU (red, green)	Blinking green	Equipment in operation
	Steady red	Device startup in progress
	Blinking red	The system software is starting and has not yet finished starting. At this point the system is in diagnostic mode and can be operated on a limited basis.
	Off	System Lock
ALM (red, green)	Off	No alarm conditions
	Blinking red	Indicates that the following problems may occur: • Device IP address conflicts with IP addresses of other devices on the LAN • Network failure • The application has exited (the device is unusable)
	Steady red	Device startup failure
SD	Steady green	Link is connected but no service flow
	Blinking green	With business flow transmission
	Off	Cardless
ETH1/ETH2 (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

 Copyright © Redstone Systems, Inc

	Shiny green on the left side	Physical links have been established and there is a business flow
	Left side off	No physical link established

Figure 1-16 REX1000 rear panel



Table 1-18 REX1000 Interface Description

Connector	Definition
RST	Restore the factory default settings of the device. Press this button with a pointed object for more than 3 seconds until both the STU and ALM indicators are green and always on, then release it and wait for the device reboot to complete.
CON	The configuration port (CON) is used for local management and debugging.
WAN/AUX/EXP1/EXP2	4 Gigabit Ethernet ports, WAN interface default IP address 10.20.2.240, AUX, EXP1, EXP2 three interfaces share a common IP address by default, the default address is 192.168.2.2. The IP address can be modified in "Basic Configuration > Network".
SD	SD card interface.
	AC power input connector for 100V to 240V alternating current (AC) voltage.
	Grounding post.

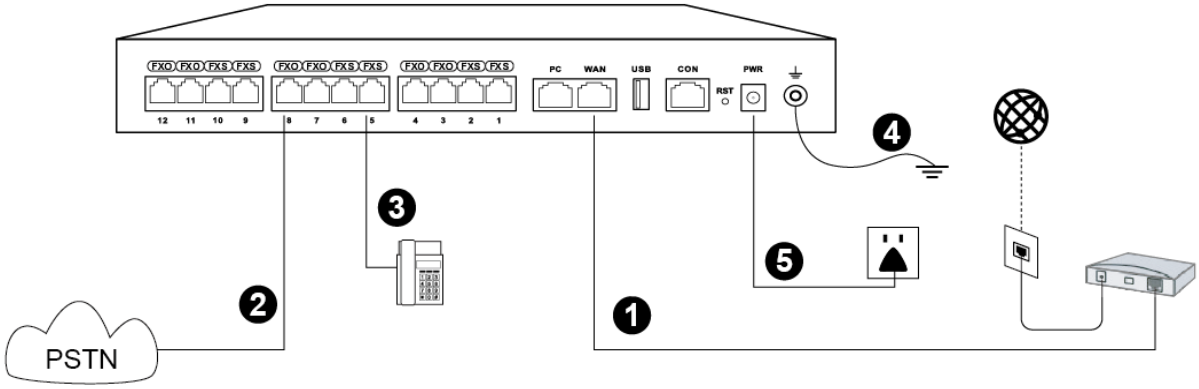
 Copyright © Redstone Systems, Inc

1.3 Access to Equipment

1.3.1 Connected device

Place the device on a flat table, or fix it in a rack, and then connect it as follows (the connection diagram takes REX50 as an example):

Figure 1-17 Installation wiring diagram



Step 1 The WAN interface (REX20/REX50/REX1000) or ETH1 interface (REX200/REX200-A/REX500) of the device accesses the network.

Step 2 The FXO interface of the device connects the telephone line provided by the telecommunication operator or other extension lines derived from the PBX.

Step 3 The unit's FXS interface connects to an analog phone or fax machine.

Description:

The FXO and FXS interfaces (RJ45) of the REX200/REX200-A/REX500 need to be wired after splitting the connected-out network cable into 4 pairs of analog telephone cables (RJ11). For RJ45 pinout specifications see Table 4-2.

REX1000 without FXO interface and FXS interface, Step 2 and Step 3 are omitted.

Step 4 The smaller diameter end of the ground wire connects to the equipment and the other end connects to the grounding strip.

Step 5 Access to power.

1.3.2 Login Device

Step 1 Connect the computer and device PC interface (REX20/REX50) or ETH2 interface (REX200/REX200-A/REX500) or AUX interface (REX1000) with a network cable.

Step 2 Queries the device IP address.

 Copyright © Redstone Systems, Inc

The REX20/REX50 factory defaults to obtain an IP address automatically via DHCP, the REX200/REX200-A/REX500 factory defaults to use the fixed IP address 192.168.2.240, and the REX1000 factory defaults to use the fixed IP address 192.168.2.2. It can also be accessed as follows:

- Get it by dialing "###" from an analog phone connected to the FXS port of the device.
- If there is no FXS port on the device (e.g. model REX20-4FXO), use the Redstone IP address acquisition tool "Finder" to obtain an IP address.

Additional Notes:

- If you need to change the device address to a fixed IP, use the analog phone to dial *90 + IP address + # subnet mask # gateway address #0#, where the "." in the IP address is replaced by "." "." in the IP address is replaced by "*". Restart the device when you hear the voice prompt "Business Registration Successful".
- If you need to configure the device to obtain an IP address through DHCP, dial *90###1# from an analog phone and restart the device when you hear the voice prompt of "successful business registration".

Step 3 Set the IP address of the computer to be in the same network segment as the IP address of the device.

Step 4 Enter the IP address of the device (e.g. 192.168.2.240) in the address bar of your browser to open the login screen.

Step 5 Select your identity and language on the login screen and enter your password to log in to the device. The default administrator password is Restone@123.



- Access to the device with HTTP is automatically switched to access via HTTPS. Since the certificate provided by the factory is used, for example, in Internet Explorer, the prompt "There is a problem with the security certificate of this website" appears, and the login page can be accessed after clicking "Continue to browse this website".
- You can't log out by closing the browser directly, you need to click "Log out" in the upper right corner of the web interface.

 Copyright © Redstone Systems, Inc

Figure 1-18 Login screen



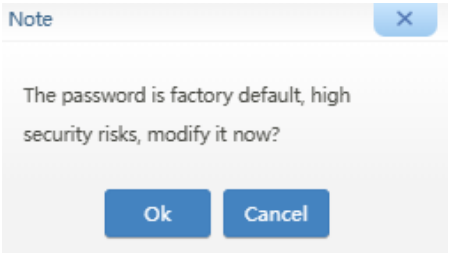
Table 1-19 Login Interface Parameters

Item	Definition
Chinese|English	Select the interface in Chinese or English.
Dignity	The device provides two levels of administrative privileges: • Administrator: has the authority to modify all configuration parameters, such as changing the login password. After logging in, "Administrator" is displayed in the upper left corner of the interface. • Operator: only has permission to view some of the parameters. After logging in, "Operator" is displayed in the upper left corner of the screen. The device allows multiple logins. When more than one person logs in with an administrator account, only one person can be the administrator, and all others are "users", and "User Browsing" is displayed in the upper left corner of the interface after logging in. Later administrators logging in can force the first logged in to log out, or not (then the later logged in logs in with user rights). Only the administrator has modification privileges. Users only have browsing privileges. Notes: The "User Browsing" mode and operator account login do not allow you to modify the configuration, and you can only browse some of the pages. The pages that cannot be viewed are: Security Configuration, Change Password, Software Upgrade, Configuration Import, and Configuration Export. It is also not possible to view the password of the IP outside line, the password of the extension and its PIN code.

Item	Definition
Pssword	The initial password for the REX20/REX50 administrator is a random password, see the label on the back of the unit. The default password for REX200/REX200-A/REX500/REX1000 is Restone@123 The default operator password is operator Change the administrator password when logging in to the device for the first time, as detailed in 02.10.5 Change Password.
CAPTCHA	Consists of 4 digits and letters. If the CAPTCHA image is not visible, you can click to change it.
Related Apps Download	Turn on the Newlync cloud service, as detailed in the Newlync Deployment Guide.

After the user logs into the page as anadministrator, a dialog box pops up prompting to change the initial administrator login password.

Figure 1-19 Prompt to change the administrator login password screen



1.4 Introduction to Web Management Interface Layout

The REX's Web management interface is divided into a system button area, a menu bar, and a configuration area.

Figure 1-20 Web Management Interface

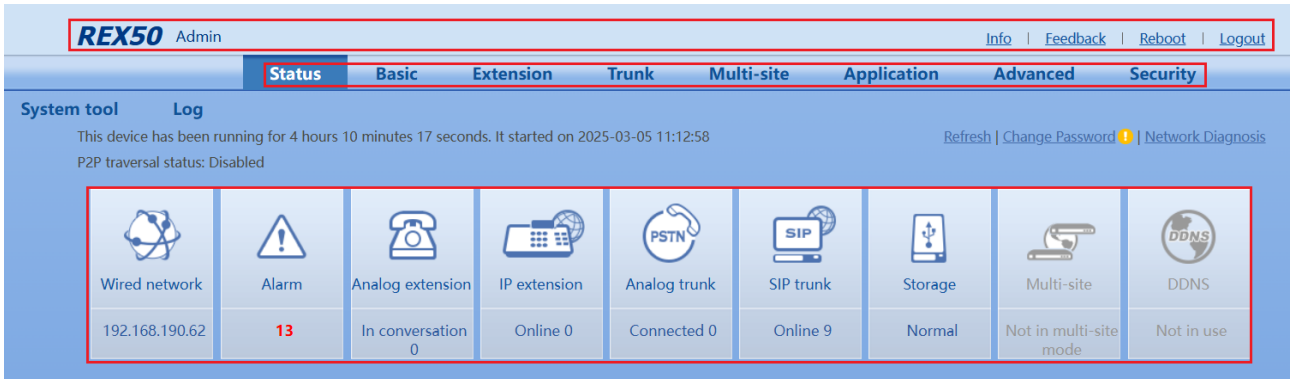


Table 1-20 Web Interface Layout Description

Item	Definition
(1) System key area	Provides buttons for Restart, Exit, Feedback, and Product Information, as well as a search box for searching the corresponding configuration page according to the function name, and displays the user identity of the current login screen.
(2) Menu bar	Mouse over the corresponding module will expand the lower-level function menu for you to choose. The selection result is displayed in the configuration area.
(3) Configuration area	Used to modify and or view the configuration.

1.5 Network Configuration

1.5.1 Network Parameters (REX20/REX50)

Click Basic Settings>Network to set the IP address and related parameters of the device according to the network environment in which the device is located.

By default, the network interface PC interface and WAN interface of REX20/REX50 are switched interfaces and share a common IP address, which is obtained through DHCP by default, and the default address 192.168.2.218 is used when DHCP acquisition fails. This address can be modified under Basic Settings>Network>WAN.

The operating mode of the PC interface can also be modified under Basic Settings>Network> PC, for a description of the parameters see Table 2-16.

 Copyright © Redstone Systems, Inc

Figure 1-21 Network Configuration Interface

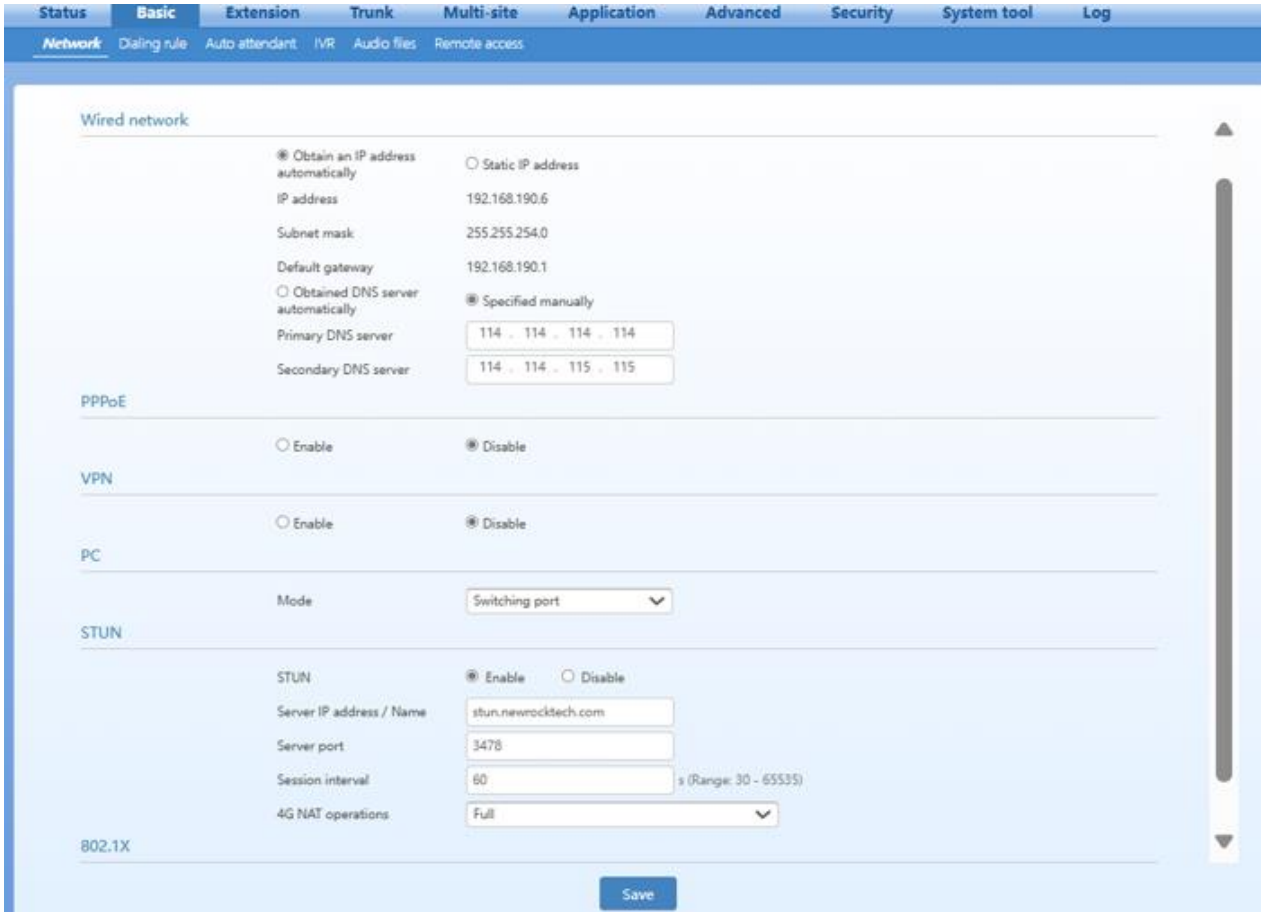


Table 1-21 Description of network parameters

Item	Definition
Wired network	● Use Dynamic Host Configuration Protocol (DHCP) to obtain IP addresses and other network parameters.
Setup	IP Address: the IP address of the device. When the connection mode is "Fixed IP Address", the address can be set manually; when the connection mode is "Automatic IP Address", the address can not be set manually, but if the automatic acquisition of the address fails, the device will use the existing fixed IP address. Subnet Mask: The subnet mask is used in conjunction with the IP address. This parameter must be entered when the gateway adopts a fixed IP address; when the IP address is obtained automatically through DHCP, the subnet mask obtained automatically by DHCP is shown here. Default Gateway: the IP address of the LAN gateway where the gateway is located. When the gateway obtains an IP address through DHCP, the LAN gateway address automatically obtained through DHCP is shown here. There is no default value for this item. DNS servers: set the preferred and alternate DND servers. Prioritize the use of preferred DNS servers to resolve domain names.
PPPoE	
User name	Enter the account number provided by your service provider. No default value.

 Copyright © Redstone Systems, Inc

Item	Definition
Password	Enter the password provided by your service provider. No default value.
DNS server	Select Obtain DNS servers automatically to obtain DNS servers from the upper router. Select Manually Configure DNS Servers to configure the preferred DNS servers and alternate DNS servers.
PC	
Operating mode	The following two modes can be configured: ● As a switching port: the PC interface and the WAN interface are switching ports, and the two interfaces can be used interchangeably. IP address of the shared WAN interface. This is the factory default configuration. ● As a dedicated interface for IP outside line (configurable IP address): This mode is generally used for PC interfaces connected to an ONU (Optical Network Unit) to access to the carrier's voice private network. If the cloud server, auto management ACS server, CDR server, API application server, and recording server are also in the dedicated voice network, you need to check the corresponding check boxes.
IP address	The IP address of the PC interface.
Subnet mask	The subnet mask of the PC interface.
Default gateway	The IP address of the LAN gateway where the PC interface is located.
Vpn	
User ID	Set the VPN account username.
Password	Set the VPN account password.
DNS server	The following two modes can be configured: ● Automatic acquisition of DNS servers: The system automatically configures DNS server addresses. ● Manual Configuration: Preferred DNS servers and alternate DNS servers are set by the user.
Stun	
Operating mode	The following two modes can be configured: ● As a switch port: the user sets the STUN server as a switch port. ● As a dedicated connection port for IP outbound (configurable IP address): Users set STUN Server as a dedicated connection port for IP outbound, and can add other applications (automatic management, CDR server, API application, recording server, and customize the IP address of STUN Server), and the connection method can be selected from fixed IP address (set by users with IP address, subnet mask, default gateway, preferred DNS server and alternate DNS server) and automatic IP address acquisition.
802.1x	Enable or disable 802.1X network port authentication.

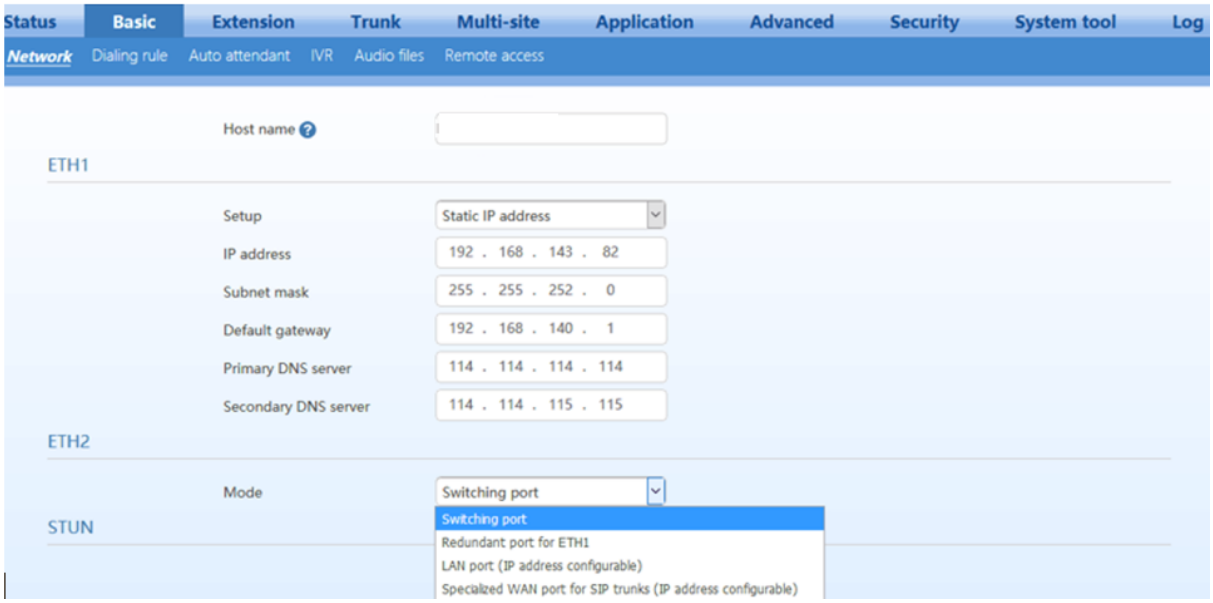
 Copyright © Redstone Systems, Inc

1.5.2 Network Parameters (REX200/REX200-A/REX500)

By default, network ports ETH1 and ETH2 of REX200/REX200-A/REX500 share the IP address of ETH1 (default 192.168.2.240) under Basic Settings>Network, which can be modified. The IP address description of ETH1 is the same as that of Table 1-21 with the WAN of the ETH1.

The ETH2 port can be modified for the network port mode. For a description of each model, see Table 1-22.

Figure 1-22 ETH2 Configuration Interface



 Copyright © Redstone Systems, Inc

Table 1-22 ETH2 Parameter Description

Item	Definition
Setup	The following four modes can be configured: ● As a switching port: ETH2 and ETH1 are switching ports, sharing the IP address configured at ETH1. This is the factory default configuration. ● As a redundant port of ETH1 port: connect both ETH1 and ETH2 interfaces to the same LAN or WAN, prioritize the use of ETH1 port, and when the ETH1 connection fails, the device automatically enables the ETH2 port (about 1.75 seconds). ● As an intranet port (configurable IP address): The ETH2 can be configured with an independent IP address for downlinking to IP phones or other Voice over IP devices. The downlink voice equipment only needs to set an IP address in the same network segment as ETH2 to interconnect with REX, which does not need to occupy the IP resources of the uplink network, reduces the load of the uplink network equipment, and the failure of the uplink network equipment does not affect the communication between REX and extensions. This mode is applicable when the IP address resources of the uplink network of the REX are tight: even if the uplink network can only assign one IP address to the REX side, the REX can still extend other voice devices. ● As a dedicated interface for IP outside line (configurable IP address): This mode is generally used for the ETH2 interface to connect to the ONU (Optical Network Unit) to access to the carrier's voice private network. If the cloud server, auto management ACS server, CDR server, API application server, and recording server are also in the voice private network, you need to check the corresponding check boxes.
IP address	The IP address of the ETH2 interface when the operating mode is set to Intranet Interface or IP Outbound Private Interface.
Subnet mask	The subnet mask of the ETH2 interface when the operating mode is set to Intranet Interface or IP Outbound Private Interface.
Default gateway	The IP address of the LAN gateway where the ETH2 interface is located.

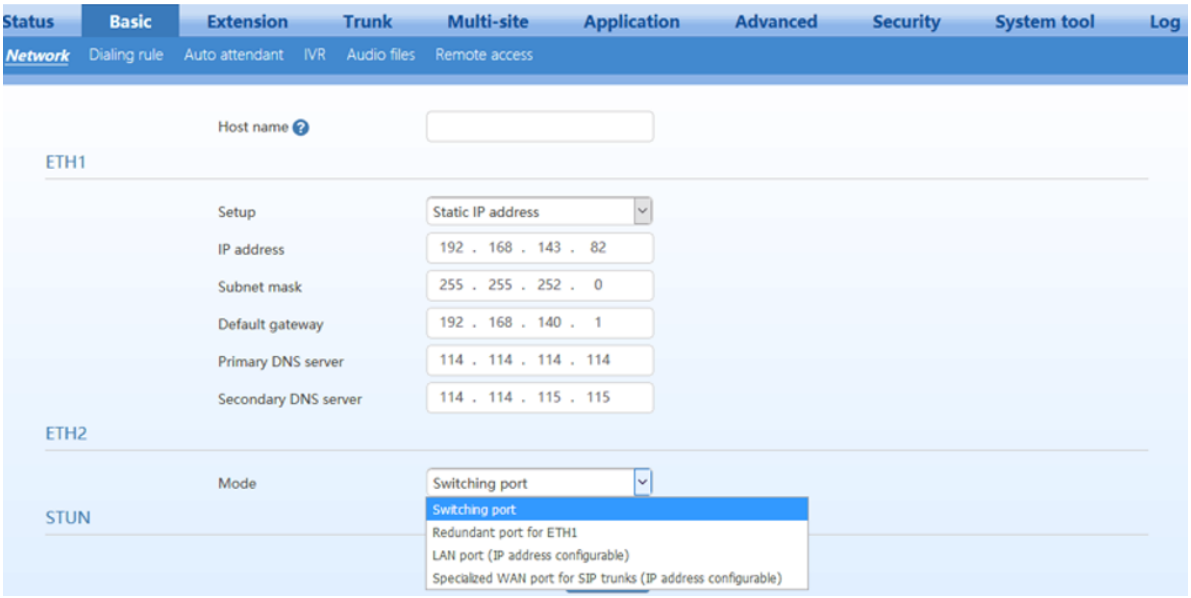
 Copyright © Redstone Systems, Inc

1.5.3 Network Parameters (REX1000)

By default, the default IP address of the WAN interface of REX1000 is 10.20.2.240 and the default IP address of the AUX/EXP1/EXP2 interface is 192.168.2.2. The IP address description of the WAN interface is the same as the Table 1-21 the WAN interface.

The AUX&EXP interface can modify the working mode of the network interface. For a description of each model, see Table 1-23.

Figure 1-23 AUX&EXP configuration interface



 Copyright © Redstone Systems, Inc

Table 1-23 AUX&EXP Parameter Description

Item	Definition
Operating mode	The following three modes can be configured: ● As a switching port: WAN interface, AUX interface, EXP1 interface and EXP2 interface are switching ports for each other and share the IP address of WAN. ● As an intranet connection port (configurable IP address): Independent IP addresses can be configured for AUX & EXP, i.e., AUX, EXP1 and EXP2 ports share the same IP address (WAN uses a separate IP address). This mode is generally used for these three interfaces to downlink IP Phones or other Voice over IP devices. The downlinked voice devices can interconnect with REX by simply setting an IP address in the same network segment as AUX&EXP, which does not need to occupy the IP resources of the uplinked network, reduces the load of the uplinked network devices, and the failure of the uplinked network devices does not affect the communication between REX and the extensions. Therefore, it applies when the IP address resources of the REX's uplink network are tight: even if the uplink network can only assign one IP address to the REX side, the REX can still extend other voice devices. This is the factory default mode. ● As a dedicated interface for IP outside line (configurable IP address): This mode allows you to configure independent IP addresses for AUX & EXP, which are shared by AUX interface, EXP1 interface and EXP2 interface. This mode is generally used to connect an ONU (Optical Network Unit) to access to the carrier's voice private network. If the cloud service, auto management, CDR server, API application, and recording server are in the dedicated voice network, you also need to check the corresponding option to use this network interface.
IP address	IP address of AUX&EXP when the operating mode is set to Intranet Interface or IP Outside Line Dedicated Interface.
Subnet mask	Subnet mask of AUX&EXP when the operating mode is set to Intranet Interface or IP Outside Line Dedicated Interface.
Default gateway	LAN gateway IP address.

1.5.4 Domain name resolution

When the device accesses a destination address in the form of a domain name, it first requests a DNS server to resolve the domain name to an IP address, for which it needs to configure the DNS server address.

Step 1 Click Basic Settings>Network to set up DNS servers.

 Copyright © Redstone Systems, Inc

Figure 1-24 DNS Server Configuration Interface

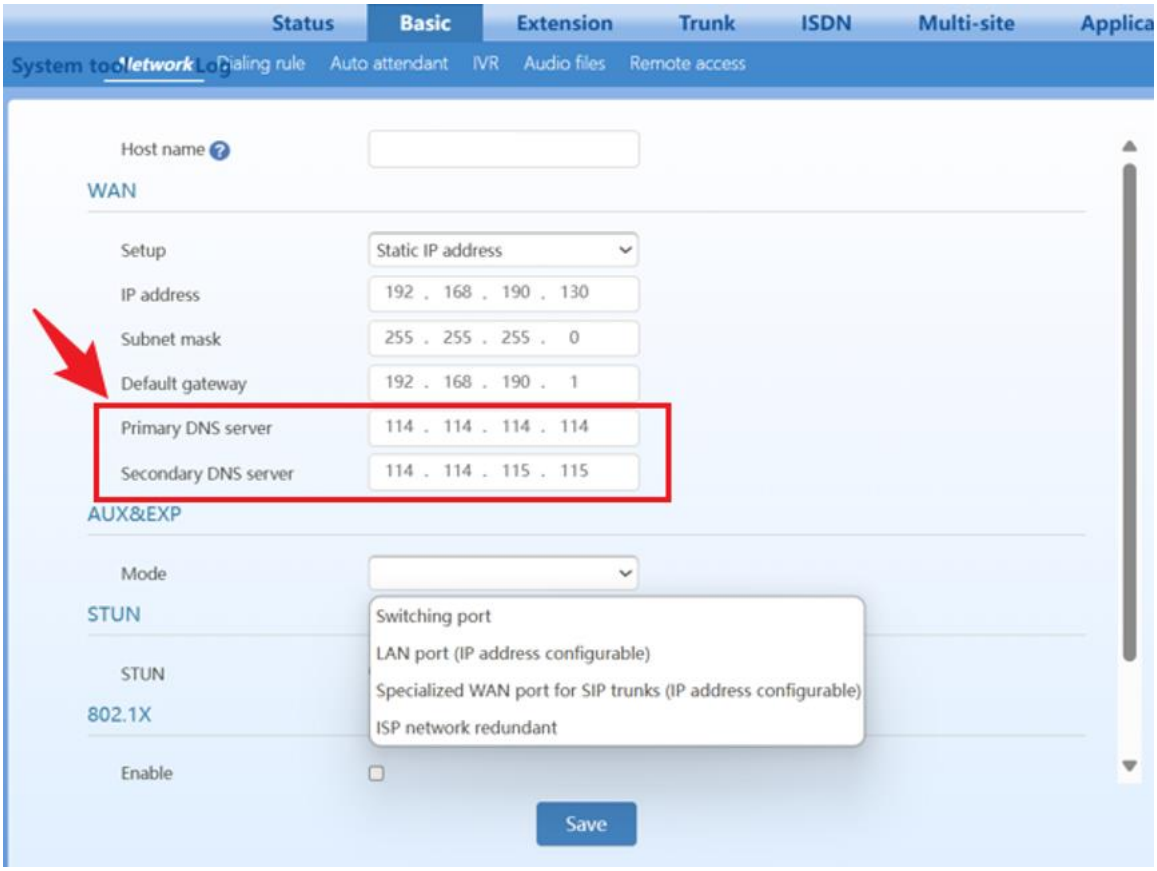


Table 1-24 DNS Server Parameter Description

Item	Definition
Auto-acquisition	The device obtains the DNS server address automatically through DHCP or PPPoE. This option can only be selected if the network connection method is configured as "Obtain IP address automatically" or "PPPoE".
Manual configuration	The device uses manually configured DNS server addresses. REX20/REX50/REX200/REX200-A/REX500/REX1000 defaults to manual configuration.
Preferred DNS servers	If you select "Manual Configuration", you must enter the IP address of the preferred DNS server for your network here, the default value for REX20/REX50/REX200/REX200-A/REX500/REX1000 is 114.114.114.114.
Alternate DNS servers	If you select "Manual Configuration", you can enter the IP address of the alternate DNS server of the network here, it is not mandatory, REX20/REX50/REX200/REX200-A/REX500/REX1000 defaults to 114.114.115.115.

 Copyright © Redstone Systems, Inc

1.5.5 STUN

Click Basic > Network to configure to obtain the public IP address of the router on the front end of the device through the STUN function.

Figure 1-25 STUN Configuration Interface

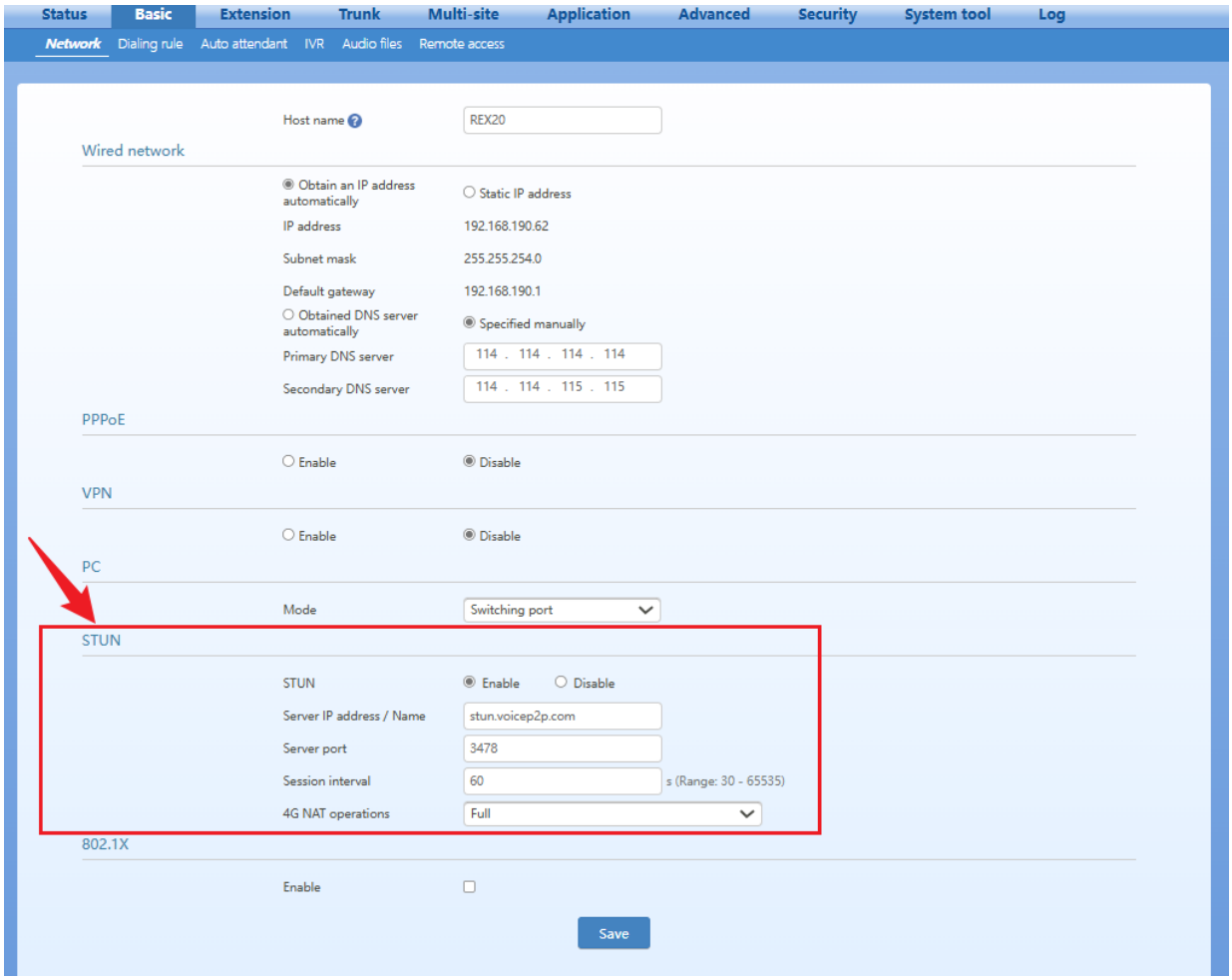


Table 1-25 Description of STUN interface parameters

Item	Definition
Stun	The device periodically sends a request to the STUN server to obtain the public IP address of the router on the front end of the device. REX20/REX50/REX200/REX200-A/REX500/REX1000 is turned on by default, and the processing is SIP re-registration.
Server IP address/domain name	Set the address of the STUN server, the factory value is the address of the Redstone Cloud server.
Server port	Set the port of the STUN server, the default is 3478.
Session interval	The interval at which the device sends STUN requests, value range 30~65535 seconds, default 60 seconds.

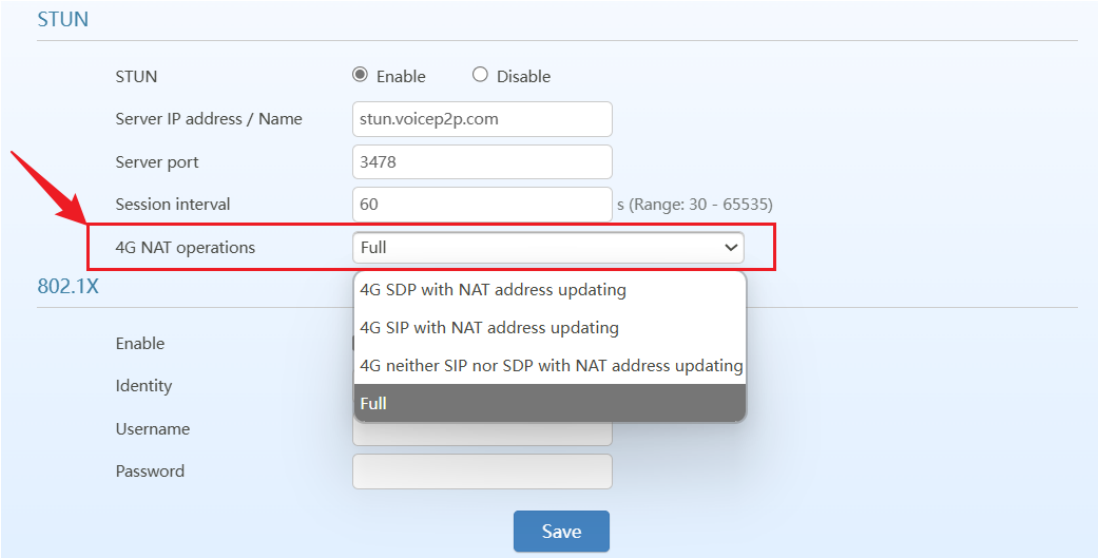
 Copyright © Redstone Systems, Inc

Item	Definition
Treatment	SIP re-registration: when there is a change in the public IP address returned by the STUN server, the device re-initiates registration with the registration server. The period for sending a STUN request should normally be less than the registration period in order to detect a change in the outside address of the router and re-register it in a timely manner. Note: The CONTACT, VIA, and "C=" domain addresses in the SIP message sent by the device remain the address of the device itself and are not replaced with the public IP address in the STUN response message. SIP re-registration + update NAT address: After the public IP address returned by the STUN server is changed, the device re-registers with the registration server and replaces the VIA, CONTACT, and "C=" domain address and port in the SDP in the SIP message.

4G NAT operations

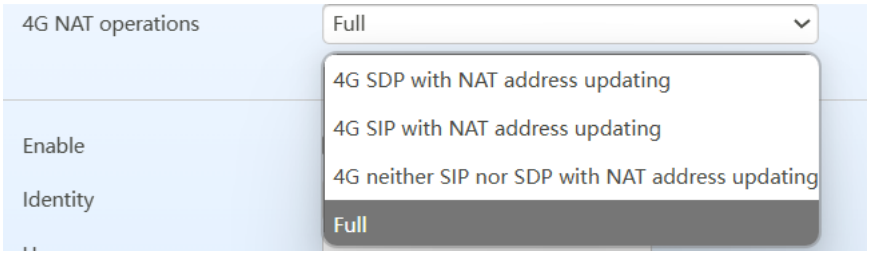
4G NAT operations, as a complementary optimization to the STUN configuration, improves the performance of REX series devices under 4G networks and ensures that communications via NAT can be smoother.

Figure 1-26 Network management interface



Step 1 Click the option box to configure

Figure 1-27 4G NAT operations options screen



Step 2 Select Configuration Options

Step 3 Save Settings

Table 1-26 Functional definition of the 4G NAT operations button

Item	Definition
Full	Enabling NAT address updates for SIP and SDP protocols.
4G SDP with NAT address updating	Update only the NAT address in the SDP.
4G SIP with NAT address updating	Update only the NAT address in SIP signaling.
4G neither SIP nor SDP with NAT address updating	No NAT address update for SIP and SDP.

802.1X

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

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

access the network.

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

Click Basic > Network to enable the 802.1X feature.

Figure 1-28 802.1X Configuration Interface

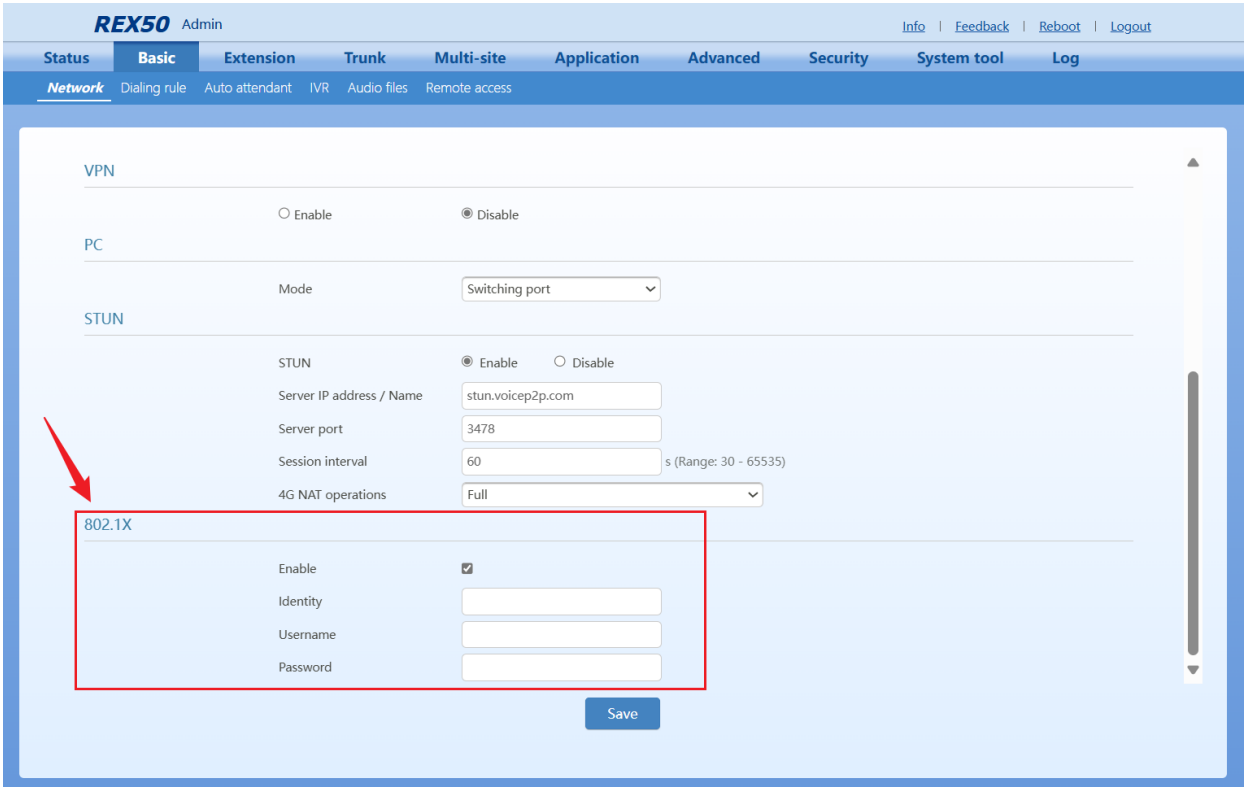


Table 1-27 802.1X Interface Parameter Description

Item	Definition
Enable	Enable the 802.1X function.
Identity	Identity for authentication, provided by the authentication server
User name	Username for authentication, provided by the authentication server
Password	Password for authentication, provided by the authentication server

1.5.6 Remote access

When the REX is behind a NAT or firewall, there are two ways to make the REX accessible to other devices or application servers on the outside network (typical application

scenarios are IP extensions on the outside network registering to the REX or multiple devices grouping together):

- Penetration method

  This method only requires that the penetration function be enabled on the REX and no other configuration is required. This is recommended as the preferred method.

- Port mapping method

  This method requires port mapping to be configured on the ingress router. you also need to configure the external network address on the REX. you may need to use DDNS.

Penetration Method

The configuration steps are as follows:

Step 1 Go to Basic > Remote access, and check the box of P2P traversal to enable it.

Figure 1-29 P2P traversal Configuration Interface

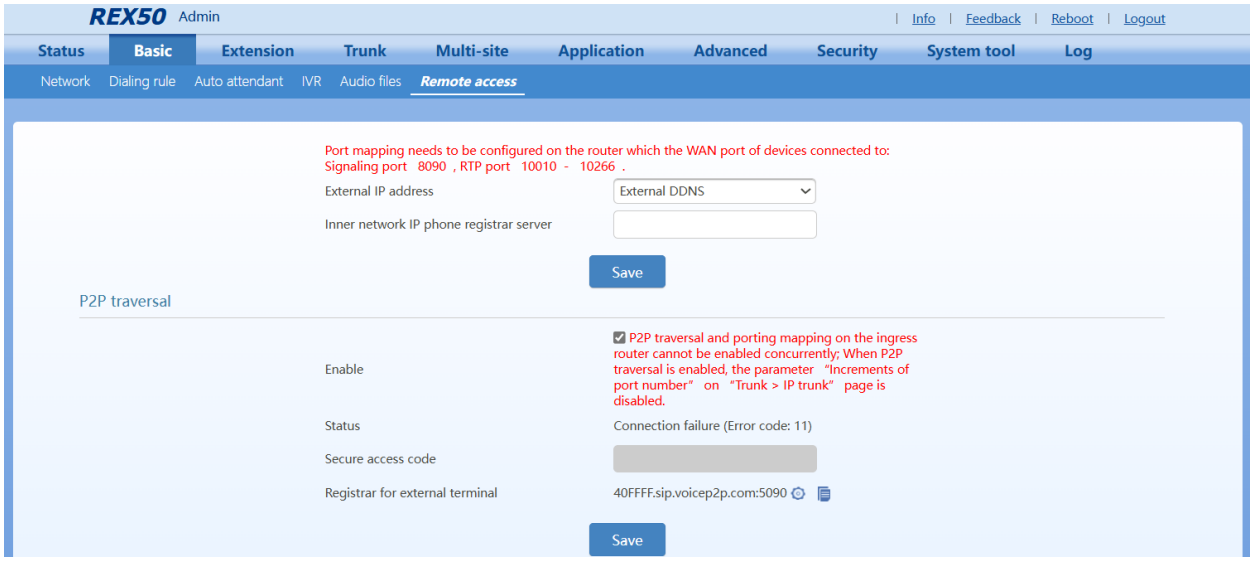


Table 1-28 Description of penetration parameters

Item	Definition
Enable	Enables or disables penetration.
Security access code	A 6-digit number randomly generated by the device. The security access code is automatically added to the followingaddresses registered for the extranet terminalsto improve the security of the domain name.
Registrar for external terminal	The penetration domain name (used by other terminals to access the REX) is automatically generated when the penetration function of the REX is enabled, and consists of the "security access code" and the "last 6 digits of the device's MAC address". Remote IP extensions only need to set the registrar server to that domain name.

Note

It is recommended to turn on the automatic detection server (configured according to the manual of the IP extension) for external IP extensions to ensure that the call-in is normal.

Step 2 Save the settings.

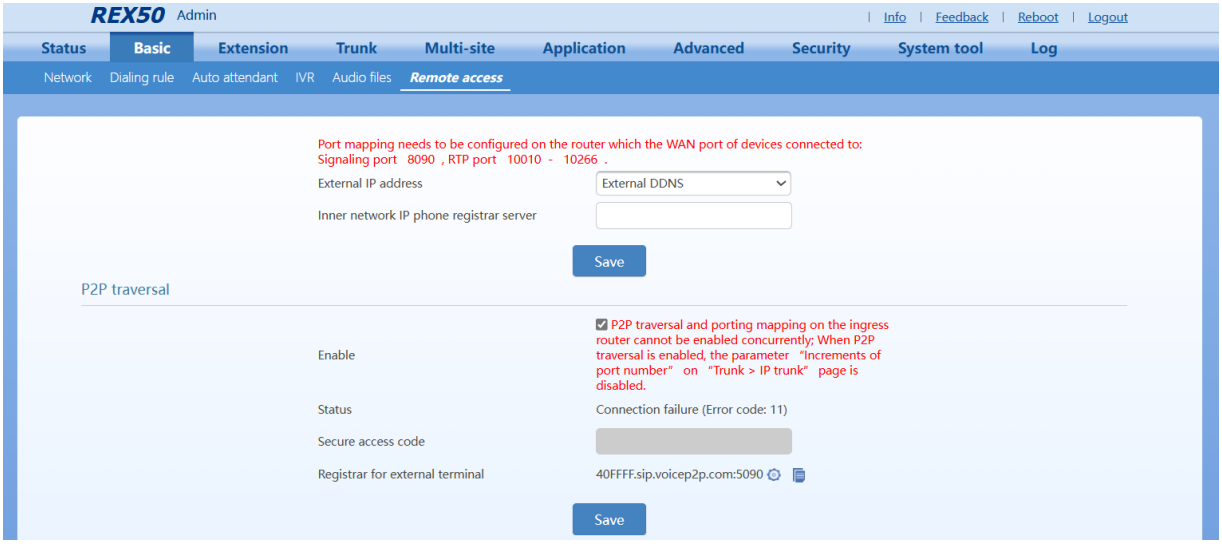
Step 3 When an external device accesses the REX, fill in the REX address as the penetrating domain name (i.e., the registered address of the external terminalon the interface).

Port Mapping Method

1. Configuring REX

Step 1 Click Basic >Remote Access to configure the remote address.

Figure 1-30 Remote Access Configuration Interface



 Copyright © Redstone Systems, Inc

Table 1-29 Description of extranet access parameters

Item	Definition
External hostname (ingress router DDNS)	Select this item when there is no fixed IP address for the external network entrance, and fill in the DDNS domain name of the WAN port of the entrance router at the domain name.
Ingress router extranet address	Select this item when the external network entrance has a fixed IP address, and fill in the public IP of the WAN port of the entrance router in the IP address field.
Built-in DDNS	This option is available when the ingress has no fixed IP address and does not use the DDNS domain name of the ingress router's WAN port. You need to apply for a domain name, username and password from a DDNS service provider. REX supports the following DDNS providers: www.oray.com, www.3322.org, dyndns.org, freedns.afraid.org, www.no-ip.com.

Step 2 Save the settings.

2. Configure the ingress router

Configure port mapping on the router, using the D-Link router as an example:

Figure 1-31 Router Port Mapping Configuration Interface



Table 1-30 Port mapping parameter

Item	Definition
IP address	Fill in the IP address of the REX. The IP address can be viewed in the Network section under the Status page of the REX. Note: The IP address of the REX needs to be the fixed IP address of the ETH1/WAN port. This address can be configured in the REX's Basic Settings>Network.
Ports	Fill in the REX's SIP signaling port and RTP port ranges. Under REX's Outside Settings>SIP Outside>Registration Options, you can view the local ports; in the Application Services>Mediapage, you can view the maximum and minimum values of RTP ports. Note: If you can specify the port number after mapping, please keep it consistent with the port number of the REX.

3. When an external device accesses the REX, the REX address filled in is the IP address or domain name of Basic Configuration>External Access>External Addresson the REX

interface.

1.5.7 VPN (REX20/REX50)

The REX20/REX50 is embedded with an OpenVPN client, which is used for SIP external access to SIP servers in a VPN network, avoiding the problems that may be caused by the SIP protocol when traversing firewalls and traversing NATs.

Note The VPN function is only used for SIP outside line access to the private LAN.

After logging in, click "Basic > Network" to configure the OpenVPN client.

Figure 1-32 VPN Configuration Interface



Table 1-31 VPN Parameter Description

Item	Definition
VPN	Select On and click Save to turn on the OpenVPN client feature. About the VPN server setup and configuration of this article is omitted. Note: The OpenVPN feature requires accurate system time, which can be checked or calibrated by going to the System tool> System time page.
OpenVPN Client Certificates	1. Prepare the OpenVPN certificate file "client.ovpn". The file should be provided by the server or created by yourself based on the information provided by the server, for details see 4 OpenVPN Certificate Creation. 2. Select the file and click "Upload". You can view the uploaded certificates in "Advanced Settings > Certificates". 3. Reboot the device. After the reboot is complete, you can view the results of the VPN connection in "Basic Configuration > Running Status".

2 Features

2.1 Auto Attendant

2.1.1 Configuring the Auto Attendant

The Auto Attendant function is the REX's ability to play voice navigation (welcome message) to the caller after an incoming call from an outside line (analog outside line, SIP outside line) is connected. Voice navigation in REX is divided into two categories: single-level voice navigation (subsequently referred to as a "voice file") and multi-level voice navigation (subsequently referred to as "multi-level IVR").

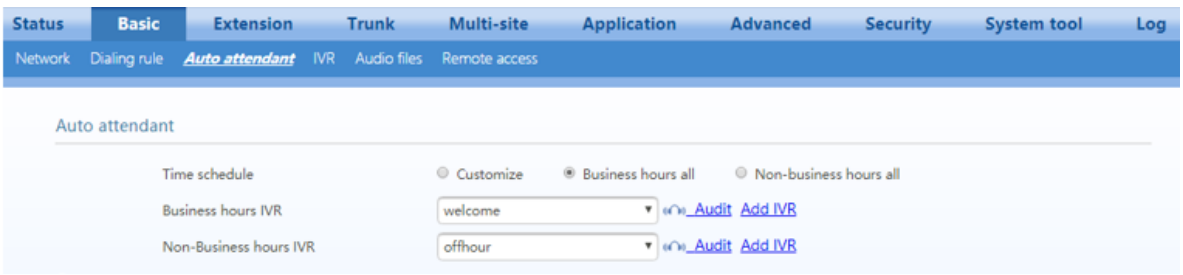
Follow the steps below to configure the voice navigation used by the automated attendant:

Step 1 Click Basic >Auto attendant to enter the Auto Attendant Configuration screen.

Step 2 Split between working and non-working hours (default is full working hours).

Step 3 Select the appropriate voice navigation for working hours and non-working hours.

Figure 2-1 Auto Attendant Configuration Screen



 Copyright © Redstone Systems, Inc

Table 2-1 Automated Operator Parameters

Item	Definition
Time schedule	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. Full work: always play the work hour welcome message. Full break: always play the welcome message during non-working hours.
Business hours IVR	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 2.1.2 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) Microphone recording welcome message. Click Auditionto listen to the current voice navigation content.
Non-Business hour IVR	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 need to change it, you need to prepare the voice file first, see 2.1.2 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, clickAdd IVR. For specific production see 3) Microphone recording welcome message. Click Audition to listen to the current voice navigation content.

Step 4 Save the settings.

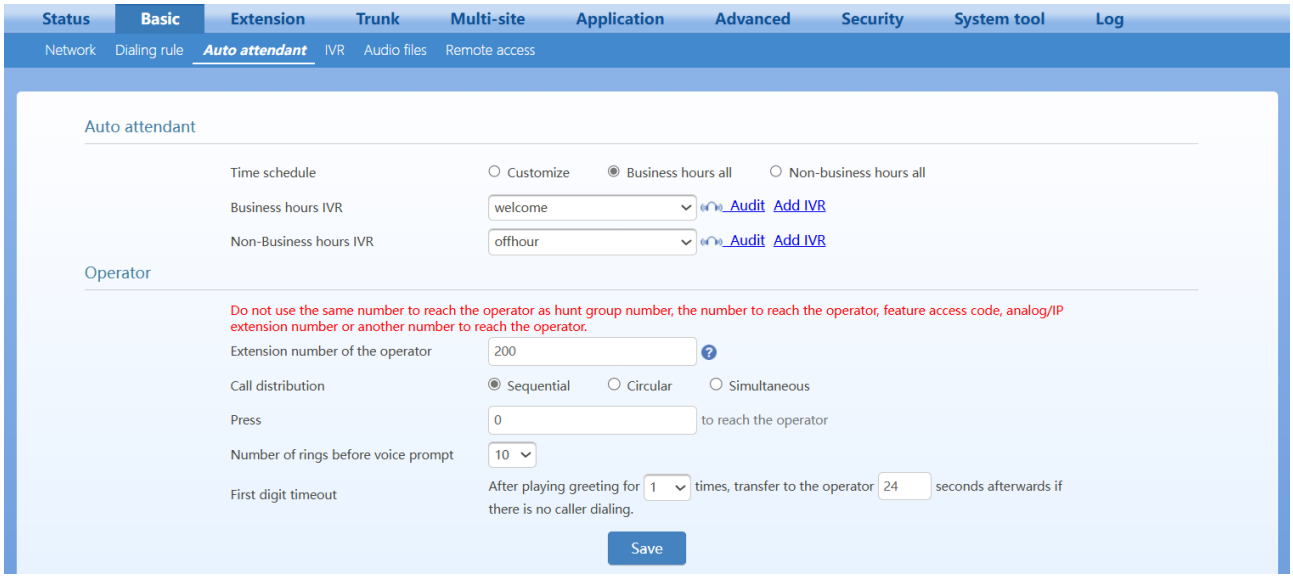


The voice navigation configured in this section is the default voice navigation used by all outside lines. If you need to change the voice navigation for an outside line individually, please go to the outside line interface to change it.

 Copyright © Redstone Systems, Inc

2.1.2 Customizing and replacing voice files

Table 2-2 The device has two voices by factory default



Time period for sth. to take effect	Voice file name	Element
Working hours	welcome	Welcome to your call, please dial the extension number directly, and dial0for number checking.
Non-Business hours	offhour	We welcome your call. It's after hours, so please dial the extension number directly.

You can also prepare voice files in the following three ways.

- Text-to-welcome message
- Microphone recording welcome message
- Upload an existing welcome message

1) Text-to-welcome message

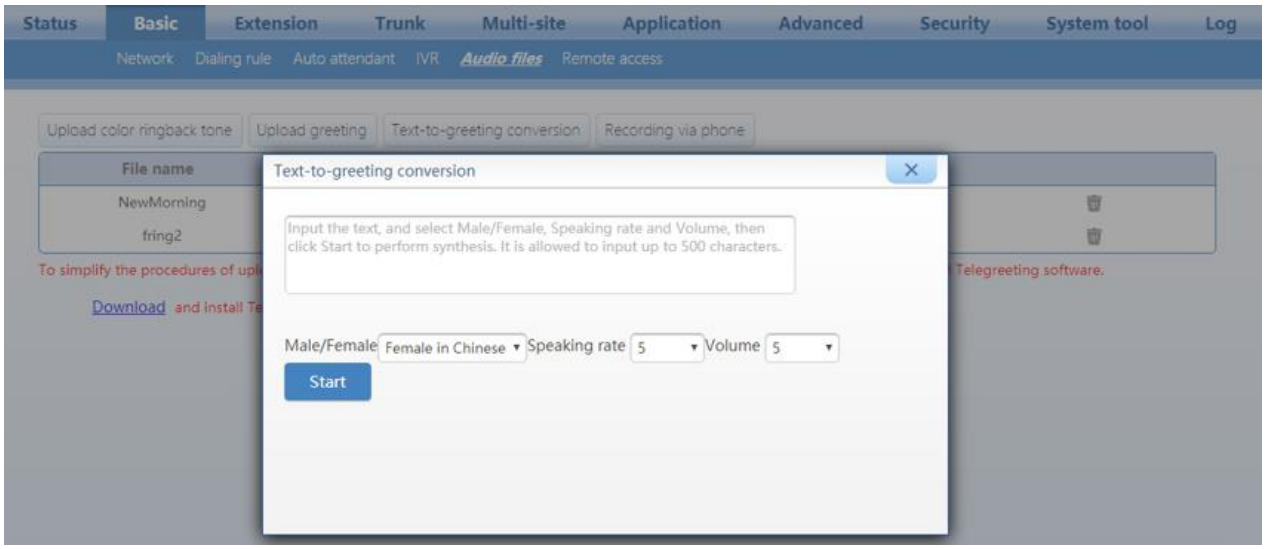
This method is easy to operate and the synthesized speech files (Chinese and English) have excellent sound quality. This option is recommended if the device has access to the Internet.

 Copyright © Redstone Systems, Inc

Step 1 Click Basic >Network to set up DNS servers, see 1.5.4 Domain Name Resolution for details.

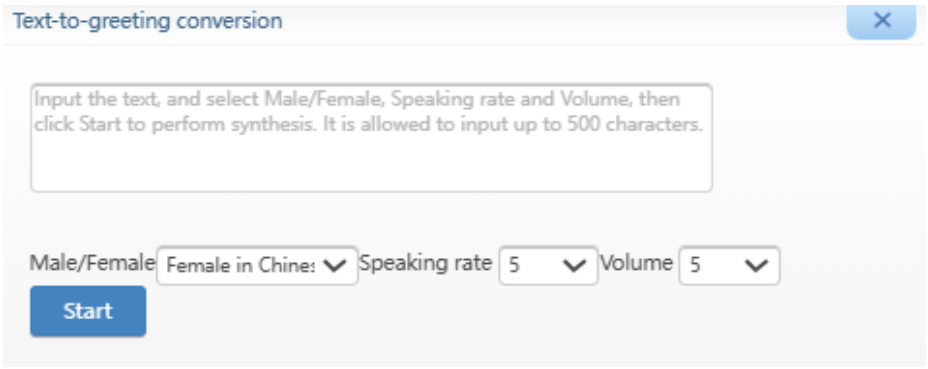
Step 2 Click Basic Settings>Audio files>Text-to-greeting conversion page to enter text and synthesize speech.

Figure 2-2 Text-to-welcome message interface



In order to get a better sound quality welcome message file, we recommend you to follow the Definition on the voice management page to download the "Wind Sound" software, and then do the text-to-welcome message operation. The operation is shown below, at this point please make sure to open the page with Firefox or Google Chrome.

Figure 2-3 Text-to-welcome message interface (after installing Wind Sound)



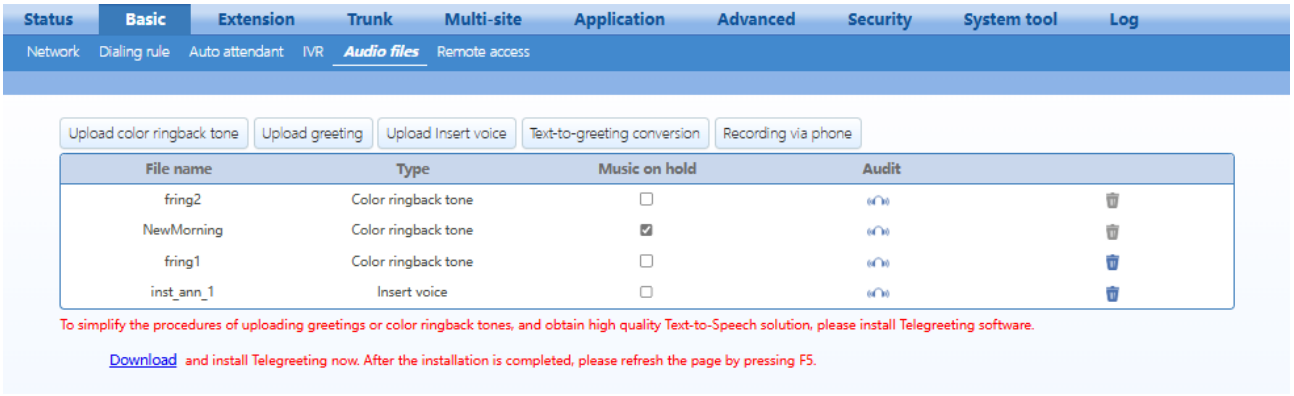
Note

The device must have normal access to the extranet when the text is transferred to the welcome message. You must also ensure that domain name resolution is turned on in Basic Settings>Network and configure the name servers.

 Copyright © Redstone Systems, Inc

Step 3 Once the sync the sized file is saved on the device, you can download it for audition and delete it on the voice management page.

Figure 2-4 Voice file management interface

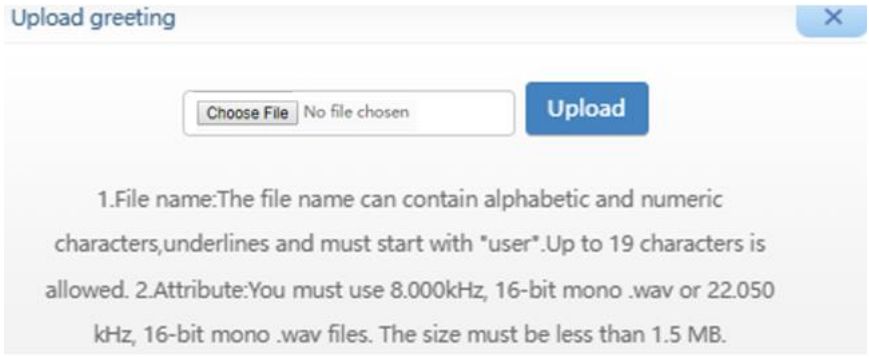


2) Upload Welcome Message

Step 1 Click Basic >Audio files> Uploading greeting.

If you don't have the voice file conversion tool "Wind Sound" installed on your computer, the page for uploading the welcome message file will be as shown below. The uploaded file must fulfill the requirements in the page.

Figure 2-5 Upload Welcome Message Screen

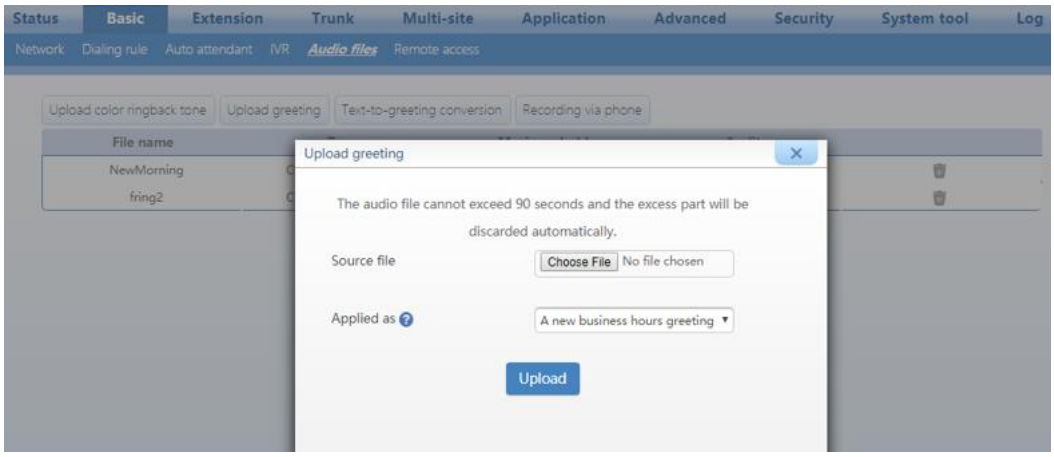


If you have not yet installed the "Voice of the wind" software, we recommend that you first download and install the "Voice of the wind" software according to the Definition on the voice management page, and then return to the page to upload the welcome message file, as shown in the following figure. At this point the uploaded file only needs to be in one of the MP3, WAV, M4A, WMA, AAC, OGG, AMR, 3GPP formats. Make sure to open the

 Copyright © Redstone Systems, Inc

page with Firefox or Google Chrome.

Figure 2-6 Upload welcome message screen (after installing Wind Sound)



3) Microphone recording welcome message

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

Table 2-3 Microphone Recording Welcome Note

Item	Definition
Recording	Take off the phone and dial *81, start recording after the voice prompt, and hang up directly after recording.
Listen	Take off the phone and dial *8200 to listen to the temporarily stored voice file.
Save	• 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.
Play the latest greeting file	• Take off the phone and dial *8201 to hear the saved work slot welcome message; • Take the machine off the hook and dial *8202 to hear a saved welcome message for non-working hours.
Recovery	Take off the phone and dial *8300 to restore the replacement of the previous voice file.

 Copyright © Redstone Systems, Inc

Note

Do not reboot the device during voice recording.

If recording with an IP extension, you must ensure that PCMU/PCMA encoding is used.

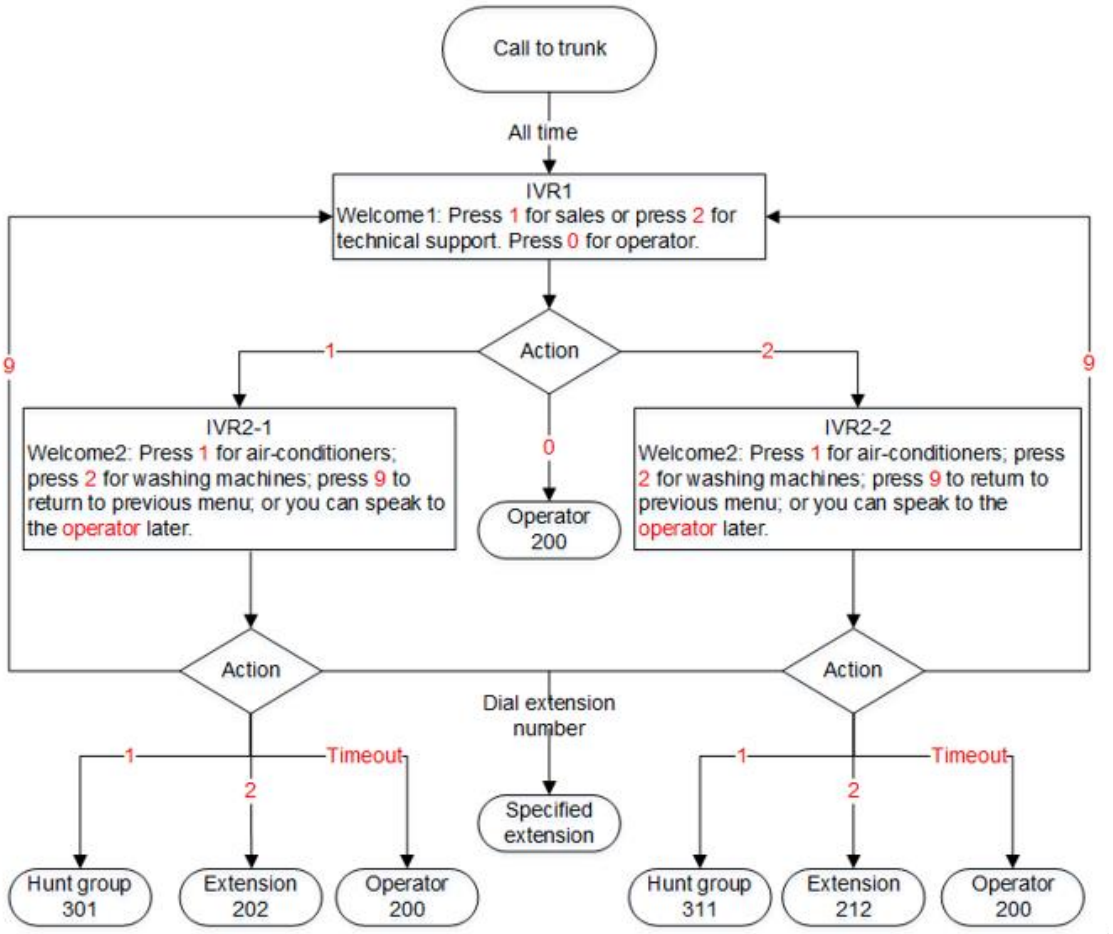
2.1.3 Creating multi-level IVR

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, and the second level corresponds to the two menus allow the user to further select "product ordering" and "technical consulting" under the sub-business respectively. 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.

 Copyright © Redstone Systems, Inc

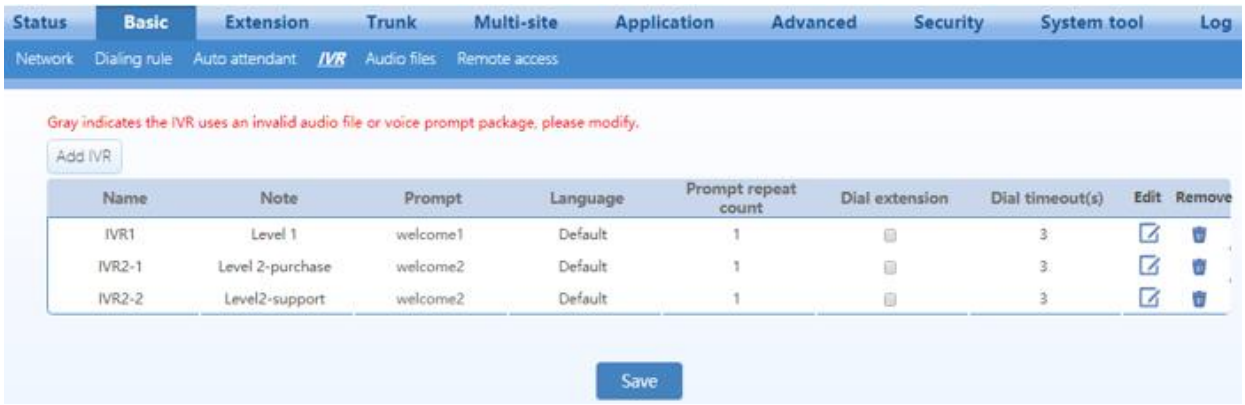
Figure 2-7 IVR Flowchart



Step 1 Prepare the voice files welcome1 and welcome2, see the above figure for the contents of the voice files, and the specific operations can be found at 2.1.2 Customizing and replacing voice files.The specific operation can be seen in the above figure.

Step 2 Click Basic >I Multi-level IVR page and click Add to create IVR1 (level 1), IVR2-1 (level 2) and IVR2-2 (level 2).

Figure 2-8 IVR Configuration Interface



 Copyright © Redstone Systems, Inc

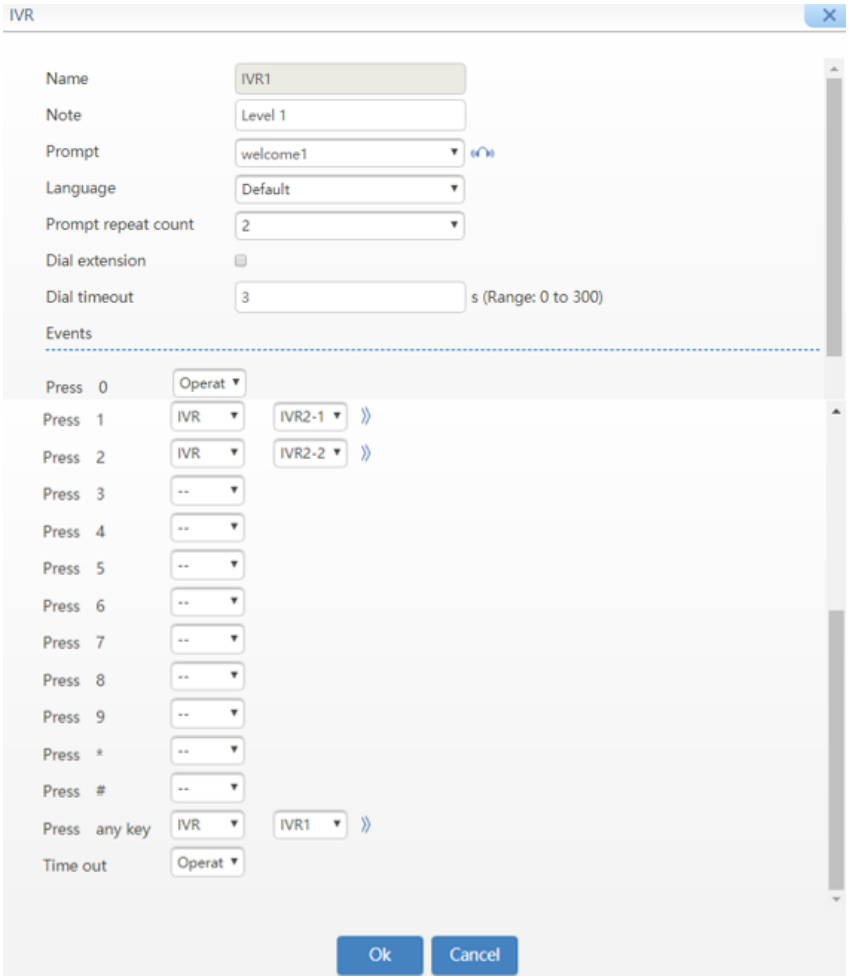
Table 2-4 IVR Configuration Interface Parameters

Item	Definition
Name	Consists of letters, numbers, hyphens and underscores, and is no more than 20 characters long.
Note	Describe the purpose of this voice navigation.
Prompt	Select the menu voice file. Voice files need to be prepared in advance.
Language	For multilingual IVR. Only if the first level menu is multilingual voice navigation, you need to select the corresponding language voice pack for each subsequent level menu. When in a single language, keep it empty and call the system's default voice prompts.
Prompt repeat count	The number of times a voice file is played without the caller dialing. The default is 1 time.
Dial extension	When checked, dialing an extension number is allowed during voice file playback.
Dial 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.

Step 3 Click Save.

Step 4 Click the Edit icon corresponding to IVR1, set IVR1 as shown below and click OK.

Figure 2-9 IVR1 Configuration Interface



 Copyright © Redstone Systems, Inc

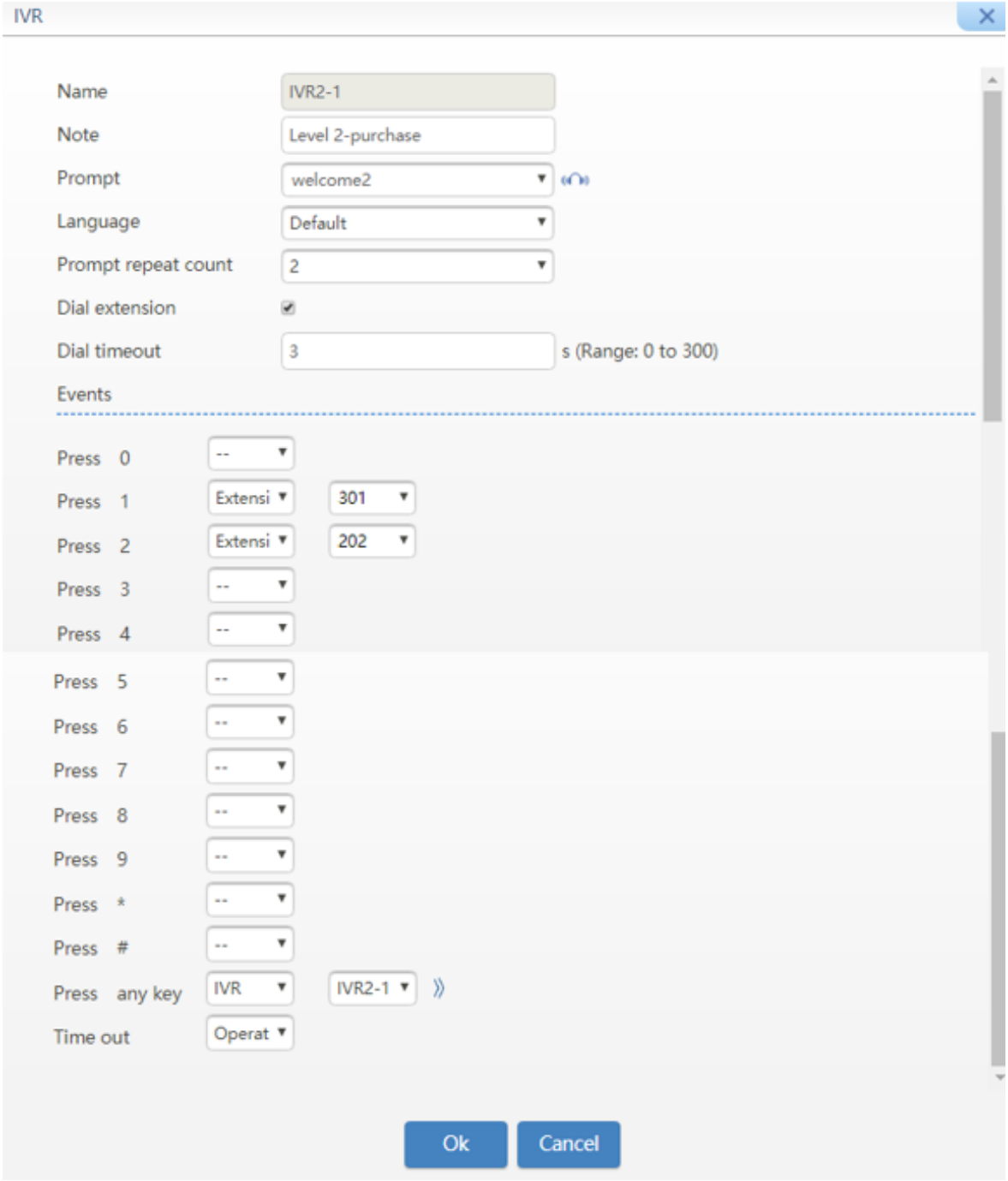
Table 2-5 IVR Menu Event Configuration Interface Parameters

Item	Definition
Event	Configure the buttons: ● 0~9, *, #: Processing after the user dials the numeric 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. Configure the operations corresponding to the keys: ● 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 an extension group (call answering group) in the Basic Settings>Dialing Rulespage beforehand, and then configure the specific key to forward to this extension group number. ● IVR: Go to the lower IVR menu and select the name of the menu that has been added to the IVR list by using the drop-down arrow. ● Hang up: ends the call. ● Operator: Transfer to an operator. The operator should be pre-configured on Basic<Auto attendant page.

Step 5 Click the Edit icon corresponding to IVR2-1, set IVR2-1 as shown below and click OK.

 Copyright © Redstone Systems, Inc

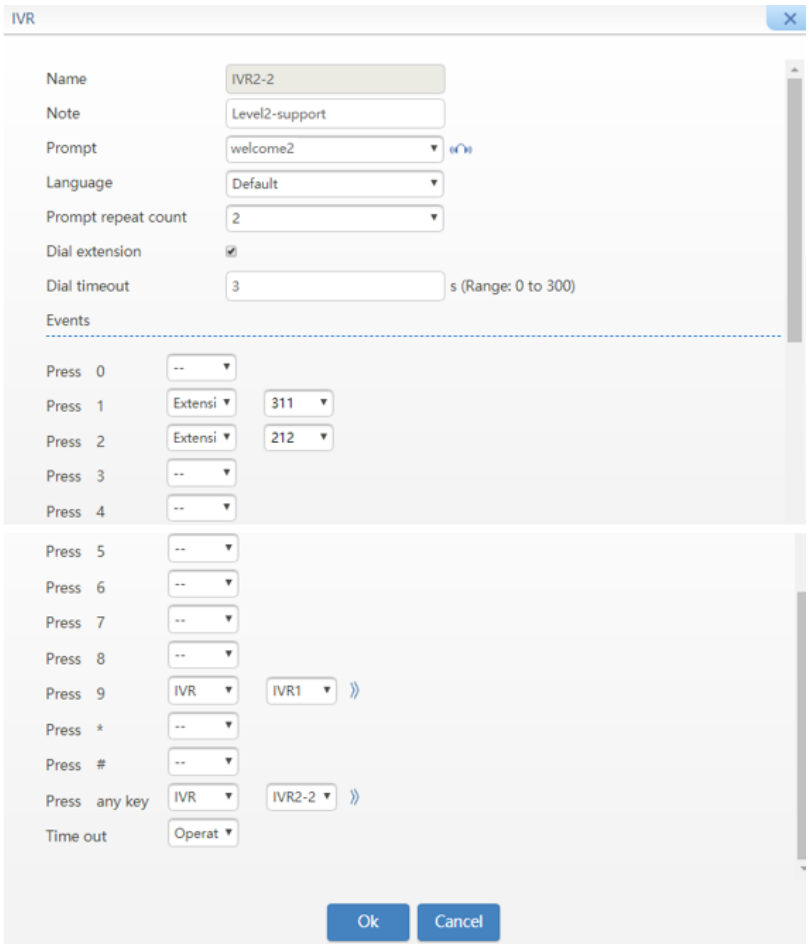
Figure 2-10 IVR2-1 Configuration Interface



Step 6 Click the Edit icon corresponding to IVR2-2, set IVR2-2 as shown below and click OK.

 Copyright © Redstone Systems, Inc

Figure 2-11 IVR2-2 Configuration Interface



2.2 Operators/Receptionists

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 called "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. The factory default operator extension is the phone connected to the first FXS port of the device. For example, if the first port of the device is an FXS port, the extension number is 200, and if the first FXS port is preceded by an FXO port, the first port number is 200, and so on. Devices without FXS ports (e.g., REX20-4FXO) have no default operator.

 Copyright © Redstone Systems, Inc

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

Step 1 Click Basic Settings>Auto attendant to configure items related to the Operator group.

Figure 2-12 Operator Configuration Screen

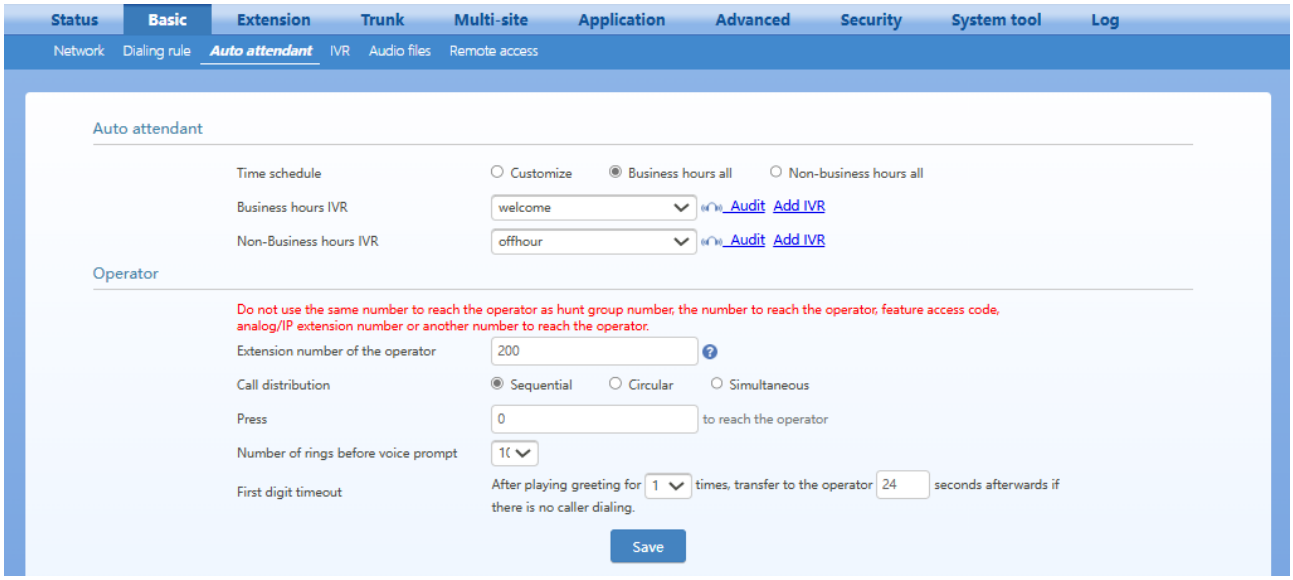


Table 2-6 Operator Parameters

Item	Definition
Extension number for the operator	Fill in the extension number of the extension acting as an operator. The default number is 200. 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. Note: Units without FXS ports (e.g., REX20-4FXO, REX50-12FXO) do not have a default switchboard.

 Copyright © Redstone Systems, Inc

Item	Definition
Call Distribution	When there is more than one operator extension, you can select the method of call distribution. ● Down Selection: Selects idle phones in the order of extension number entry in the switchboard input box. If the numbers filled in the switchboard are 321, 322, and 323, and the operator extension that is on the line is 321, the next incoming call will select 322 to ring. ● Circular: 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's extension that answered the last call is 322, then another incoming call will select 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".
Press (number) to reach the operator	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 before voice promp	When an outside caller dials an extension and the number of times the extension rings reach the set value (the default number is 10), the device plays a voice prompt to the caller.
First digit timeout	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.

Step 2 Save the settings.

 Copyright © Redstone Systems, Inc

2.3 Trunk

2.3.1 Analog Trunk (REX1000 does not have an analog external line)

The steps to configure an analog outside line are as follows:

Step 1 Connect the telephone line provided by the telecommunication carrier or the extension line leading from other PBXs to the FXO port of the REX.

Step 2 Go to Trunk>Analog trunk to configure the line.

Figure 2-13 Analog trunk Configuration Interface 1



Table 2-7 Analog Outside Line Configuration Parameters

Item	Definition
Connection status	Displays whether an analog outside line is connected to the current port.
Port	Corresponds to the FXO port serial number on the device panel.
Enable	Enabled by default. If this item is unchecked, the device will not use the analog line on this port for outgoing calls.
Number	FXO line number, defaults to 2xx. When an incoming call does not have caller ID information or the Caller ID function is not turned on, the device will use the number set here as the calling number, so it is recommended to change it to the actual number of the connected analog outside line. Note: All outside numbers cannot be duplicated, nor can outside numbers be duplicated with extension numbers.
Polarity Reversal Detection	With reverse polarity detection turned on, calls are processed in the Loop Start signaling mode if no reverse polarity is actually detected.
Inbound route	Select the access method for this outside line: • Switchboard: Incoming calls to this outside line are handled using the automatic switchboard method. • Straight Line: Binds an outside line to an extension, and when an incoming call comes in, the device bypasses the automated switchboard and delivers the call directly to the bound extension.

 Copyright © Redstone Systems, Inc

Item	Definition
Greetings	Select the voice navigation played by this outside line for incoming calls. This item can be configured only when you select the access methodas the switchboard. • Switchboard Welcome Message: Indicates the use of voice navigation configured using the Basic Settings>Audio file 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 is only played during working hours, and only the voice navigation configured in the Basic Settings>Audio file page can 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.
DID number	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.
Outbound call	When the access method for an outside line is set to switchboard, there are two types of outgoing privileges for that line: • Allow: Allows the line to be selected for outgoing calls, 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 Exclusive: This outside line is only allowed to be used when a bound extension or an extension group is calling out. And the bound extension will only use the outgoing line to go out when it makes an outgoing call, which is not affected by the outgoing call rules.
Recordings	Check the box to turn on the recording function for the outside line. Note: To enable recording, you also need to enable recording on the Application Services>Recording page, for details, see 02.6.1 Recordings.
Caller ID detection	When an external telephone calls an REX extension through an analog outside line, the number of the caller's counterpart (external telephone number) is displayed on the extension if Caller ID detection is turned on; if it is not turned on, the FXO port line number is displayed. Enabled by default.
Gain to IP	Used to adjust the volume level received on the FXO port. When talking to an analog outside party, if the extension party's answer volume is too low or too high, the parameter value can be adjusted up or down. Range: -3.0 to +9.0 dB. Note: The Gain to IP in Analog Outside > Advanced is a global configuration.
Gain to PSTN	Used to adjust the volume level sent by the device to the FXO port line. When talking to an analog outside party, this parameter can be adjusted up or down if the other party's answer volume is too low or too high. Range: -6.0 to +3.0 dB. Note: The gain to the PSTN in Analog Outside > Advanced is a global configuration.
Advanced	Sets the advanced properties of the analog outside line.

 Copyright © Redstone Systems, Inc

Step 1 Click Advanced to go to the advanced settings for the analog outside line. This page parameter relates to volume, caller ID display, and busy signal detection. If the device is used normally, there is no need to change the factory default parameters.

Figure 2-14 Analog Outside Line Advanced Settings screen

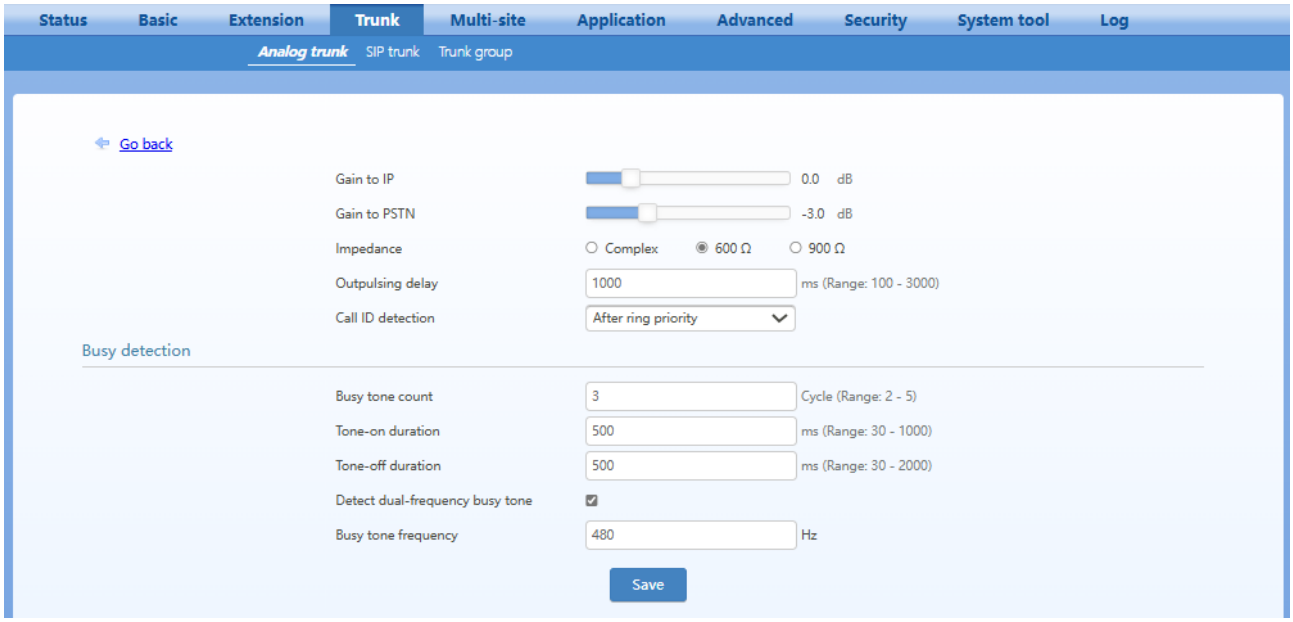


Table 2-8 Advanced configuration parameters for the proposed external line

Item	Definition
Gain to IP	Used to adjust the volume level received on the FXO port. When talking to an analog outside party, if the extension party's answer volume is too low or too high, the parameter value can be adjusted up or down. Range: -3.0 to +9.0 dB.
Gain to PSTN	Used to adjust the volume level sent by the device to the FXO port line. When talking to an analog outside party, this parameter can be adjusted up or down if the other party's answer volume is too low or too high. Range: -6.0 to +3.0 dB.
Impedance	This parameter can be adjusted when an echo is heard on the PSTN side. It is generally sufficient to keep the default values.
Outpulsing delay	The time between the FXO off-hook and the delivery of the DTMF called number. If the value is set too small, it may cause the opposite-end device to miss the number, and too large will prolong the turn-on time. It is generally sufficient to keep the default values, which are 1000 for REX20/REX50 and 600 for REX200/REX200-A/REX500.

 Copyright © Redstone Systems, Inc

Item	Definition
Incoming detection mode	The selection of the device to show the detection mode needs to be set according to the characteristics of the peer switch. ● Adaptive (after ringing priority): The first call after plugging in or unplugging the phone line or restarting the device will detect the incoming call after ringing, if the incoming call is not detected, the next call will detect the incoming call before ringing. ● Adaptive (Pre-Ring Priority): The first call after plugging in or unplugging the phone line or restarting the device will detect the incoming call before ringing, if the incoming call information before ringing is not detected, the next call will detect the incoming call after ringing. ● Before Ringing: Each call is detected to show before ringing. ● After Ringing: Each call is detected after ringing to show. The factory default is "Adaptive (After Ringing Priority)", if after plugging in or unplugging the phone line or restarting the device, there is always a situation where the first call is not detected, you can set it to "Before Ringing" or "Adaptive (Before Ringing Priority)". Priority".
Busy tone count	The number of times a busy signal is received is compared to the detection threshold, and the device ignores the received signal if it is less than the detection threshold. Range: 2 to 5 times.
Tone-on duration	• The duration of the busy signal should be set according to the busy specification of the country or region where you are located. Defaults to the Chinese busy signal specification. If US, the value of this parameter should be adjusted to 500 milli seconds. Busy tone specifications for national regions can be found in 2.9.10.
Tone-off duration	The length of the interval between busy signals should be set according to the busy specification of the country or region where you are located. Defaults to the Chinese busy signal specification. If US, the value of this parameter should be adjusted to 500 milliseconds. National or regional busy tone specifications can be referenced 2.9.10.

2.3.2 SIP Trunk

REX supports Skype Connect in addition to the standard SIP specification, which needs to be selected when making SIP outbound settings. You need to apply for an account with your VoIP operator before you can set up a SIP outbound line.

The configuration steps are as follows:

Step 1 Click Trunk > SIP Trunk.

Step 2 Click New to fill in the registration information for the new SIP outbound.

Note: If the device needs to register to multiple SIP servers (including docking to Skype connect), you need to enable multi-platform in Trunk>SIP trunk>Registration Options first.

 Copyright © Redstone Systems, Inc

Figure 2-15 SIP Outbound Configuration Interface

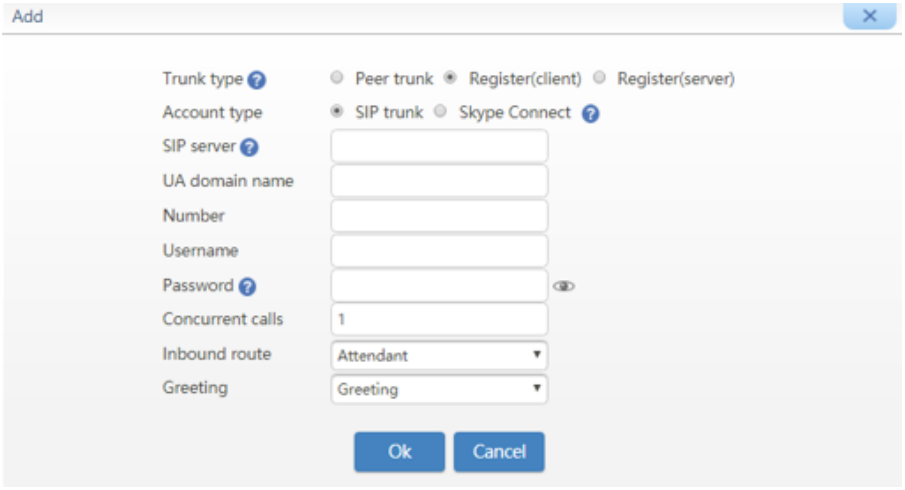


Table 2-9 Description of SIP outbound registration parameters

Account Type	Item	Definition
IP external line	SIP server	Fill in the server address and port provided by the VoIP operator. Note: When using a domain name address, the Basic Configuration > Network interface must be configured with a domain name resolution server.
	UA Domain name	Provided by VoIP carriers such as salesdepart.abccompany.com.
	Number	Fill in the outgoing number provided by the VoIP operator, e.g. 62019550185. Note: All outside numbers cannot be duplicated, nor can outside numbers be duplicated with extension numbers.
	User name	Fill in according to the requirements of the VoIP operator for the registration and authentication of the SIP outside line. If not filled in then use the number to authenticate.
	Password	Provided by the VoIP service provider. The device encrypts the IP external password by default, and you need to contact the service provider to deal with it after forgetting the password. Supports registration passwords of up to 16 characters in encrypted case (up to 30 characters in non-encrypted case).
	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 120 (200 for REX1000), and the sum of the number of concurrent calls to all outside numbers cannot exceed the maximum number of SIP outside numbers for the device. The maximum number of SIP external lines is 24 for the REX20, 62 for the REX50, 216 for the REX200/REX200-A, 496 for the REX500, and 1000 for the REX1000.

 Copyright © Redstone Systems, Inc

Account Type	Item	Definition
	Trunk type	There are three types: Direct connection: point-to-point docking. Both parties are authenticated by the filled-in IP address. Registration: the REX registers to the SIP server. Registered: the remote FXO port gateway is registered as a SIP outbound for the REX. The FXO port of the REX can be expanded. A registration username and password must be set on the REX, and the gateway will use this username and password to register to the REX.
	Inbound route	Select the access method for this outside line: • Attendant: Incoming calls to this outside line are handled using the automatic switchboard method. • DID: 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.
	Greeting	Select the voice navigation played by this outside line for incoming calls. This item can be configured only when you select the access methodas the switchboard. • Switchboard Welcome Message: Indicates the use of voice navigation configured using the Basic >Audio file. 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 is only played during working hours, and only the voice navigation configured in the Basic >Audio file can 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. a welcome message for up to 30 inbound lines at the same time.
	DID number	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.

 Copyright © Redstone Systems, Inc

Account Type	Item	Definition
	Outbound call	When the access method for an outside line is set to switchboard, there are two types of outgoing privileges for that line: • Allow: Allows the line to be selected for outgoing calls, 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.
Skype	SIP user	Authentication information in the SIP account configured on the Skype website. Please refer to the guidance document on Skype's website Skype Connect User Guide on Skype's website as a reference for the relevant parameters.
	Password	Authentication information in the SIP account configured on the Skype website. The password is displayed in ciphertext, click to display it in plain text.
	Skype connect address	Typically, sip.skype.com, which corresponds to the "Skype Connect Address" in the authentication information obtained from the Skype website. Note: You need to configure the domain name resolution server in the Basic Configuration>Network interface.
	UDP port	The default is 5060, which is consistent withthe "UDP Port" value in the authentication information obtained from the Skype website.
	Registration	You need to check the box when registering, otherwise the registration will not be successful.
	Inbound route	Select the access method for this outside line: • Switchboard: Incoming calls to this outside line are handled using the automatic switchboard method. • Straight Line: Binds an outside line to an extension, and when an incoming call comes in, the device bypasses the automated switchboard and delivers the call directly to the bound extension.

 Copyright © Redstone Systems, Inc

Account Type	Item	Definition
	Greeting	Select the voice navigation played by this outside line for incoming calls. This item can be configured only when you select the access method as the switchboard. • Switchboard Welcome Message: Indicates the use of voice navigation configured using the Basic Settings>Audio file 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 is only played during working hours, and only the voice navigation configured in the Basic Settings>Audio file page can 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.
	DID number	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.
	Outbound call	When the access method for an outside line is set to switchboard, there are two types of outgoing privileges for that line: • Allow: Allows the line to be selected for outgoing calls, 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 tostraight 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.
	Add skype number	Skype number tied to your SIP account on the Skype website, e.g. 13152880961.

Step 3 Click OK to return to the SIP Outside Line Configuration screen to view the registration status of the configured SIP outside line.

 Copyright © Redstone Systems, Inc

Figure 2-16 SIP Outbound Configuration Interface

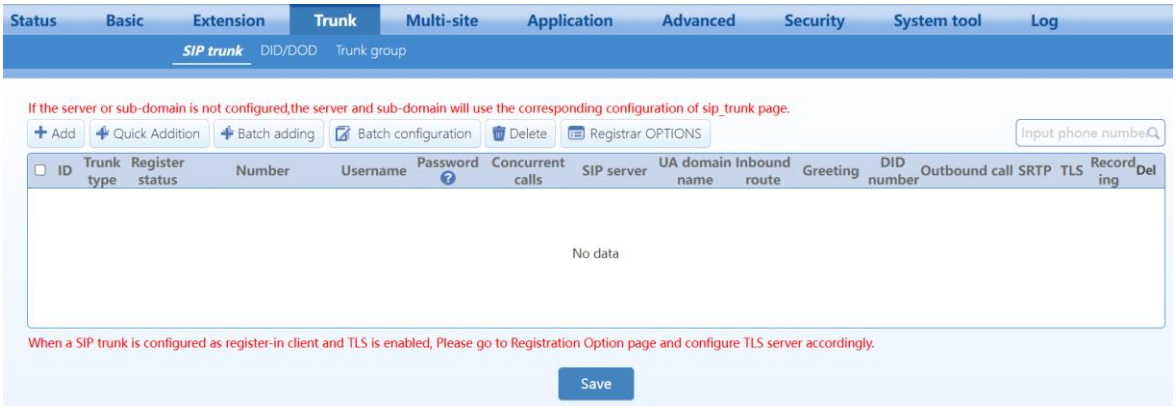


Table 2-10 SIP Outbound Interface Parameter Description

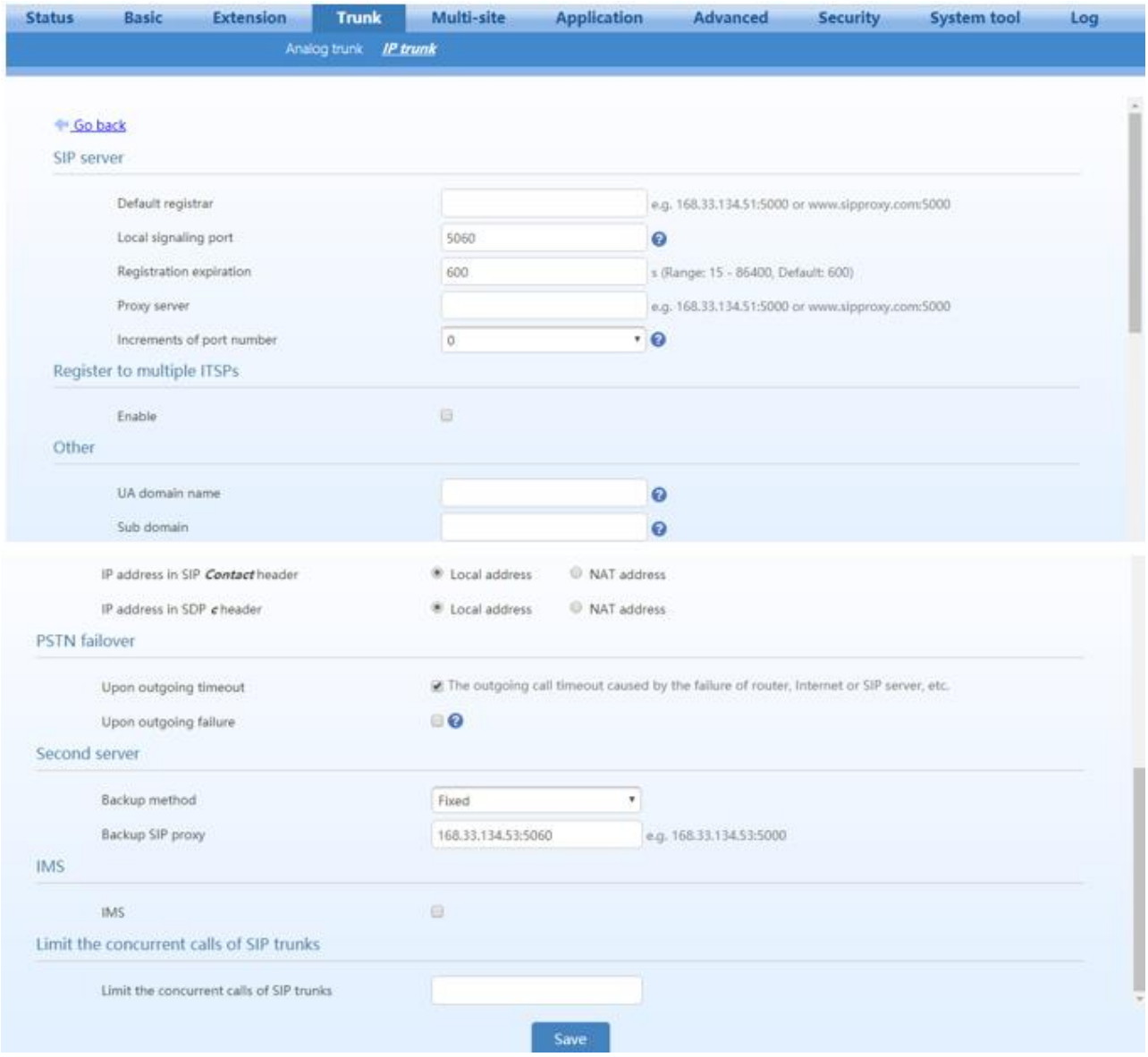
Item	Definition
ID	Line number.
Registration status	There are 5 registration statuses: • Successful registration indicates that this SIP outside line is available for use. • Registration Failure indicates that there was an error in the registration of the SIP outside line. At this time, this SIP external 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. • Domain name resolution failure indicates that the SIP outbound registration failed due to domain name resolution problem. Please check if the DNS servers are configured correctly on the Basic Configuration > Network page.
Trunk ID	See Table 2-9.
Concurrent calls	
Username	
Password	
SIP server	
UA domain name	
Registration	
Inbound route	
Greetting	
DID number	
Outbound calls	
Recording	Turn on the recording function for the outside line. Note: To enable recording, you also need to enable the recording function in the Application Services>Recording page For details, see 2.6.1 Recordings.

 Copyright © Redstone Systems, Inc

Item	Definition
Delete	The current SIP outside line can be deleted.

Step 4 Click Registration Optionsto modify the local port, registration timeout and other information. It is recommended to modify the local port to avoid SIP attacks.

Figure 2-17 SIP Outbound Registration Options Screen



 Copyright © Redstone Systems, Inc

Table 2-11 Parameter Description of SIP Outbound Registration Options

Item	Definition
Default registrater	A global parameter that is invoked to configure the SIP server address of a single line when it is not filled in. Configure the address and port number of the SIP registration server, the address and port number should be separated by ":". There is no default value for this item. 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 turn on the DNS service and configure the DNS server parameters in the Basic Configuration > Network interface.
Local signaling 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 expiration	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 the domain name form, you can fill in an alternate IP address at 2.3.3 Backup SIP Server Configuration.You can fill in an alternate IP address for the device to switch to when the domain name resolution service fails.
Increments of port number	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.
Permit to use multiple ITSP	Allows for multi-platform functionality. Once turned on, you can configure the registration server and client-side domain name for each IP outside line.
UA domain name	The attribution of the IP outbound number, provided by the SIP outbound carrier, example: abccompany.com.
Sub domain	The attribution of the IP outbound number, provided by the SIP outbound operator, is used in conjunction withthe SIP client-side domain name. If the domain name is configured as abccompany.com and the subdomain is configured as ims, the full domain name is ims.abccompany.com.
IP address in SIP Contact Header	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.

 Copyright © Redstone Systems, Inc

Item	Definition
IP address in SDP Cheader	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.
PSTN Failover	Outbound Timeout: Automatically call out from the analog outside line of the device when there is a network failure that makes the SIP outside line unavailable. Outbound Failure: when the call is delivered to the SIP operation platform and receives 4xx, 5xx and 6xx signaling (except 401/404/422), it will try to call out from the device's analog outside line. Note: The device must have an analog outside line port to use this feature.
Tls srtp	TLS Server: Set the TLS server address. TLS Backup Server: Set the TLS backup server address. SRTP Mode: select SRTP mode, there are 5 modes: outbound RTP only negotiation, inbound preferred RTP; outbound SRTP negotiation, inbound preferred SRTP; outbound RTP+SRTP negotiation, inbound preferred RTP; outbound RTP+SRTP negotiation, inbound preferred SRTP; mandatory. TLS Side Server: Check to enable TLS side server.
Limit the concurrent calls of SIP trunks	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.

2.3.3 Backup SIP Server Configuration

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: Primary server refers to the proxy server configured in Outbound Settings>SIP Outbound>Registration Options. Other SIP servers configured for SIP extranets after the multiplatform is turned on do not support the backup mechanism.

The backup server configuration steps are as follows:

Step 1 Click Trunk > SIP Trunk > Registration Options to find the backup server configuration.

Figure 2-18 Backup Server Configuration Interface

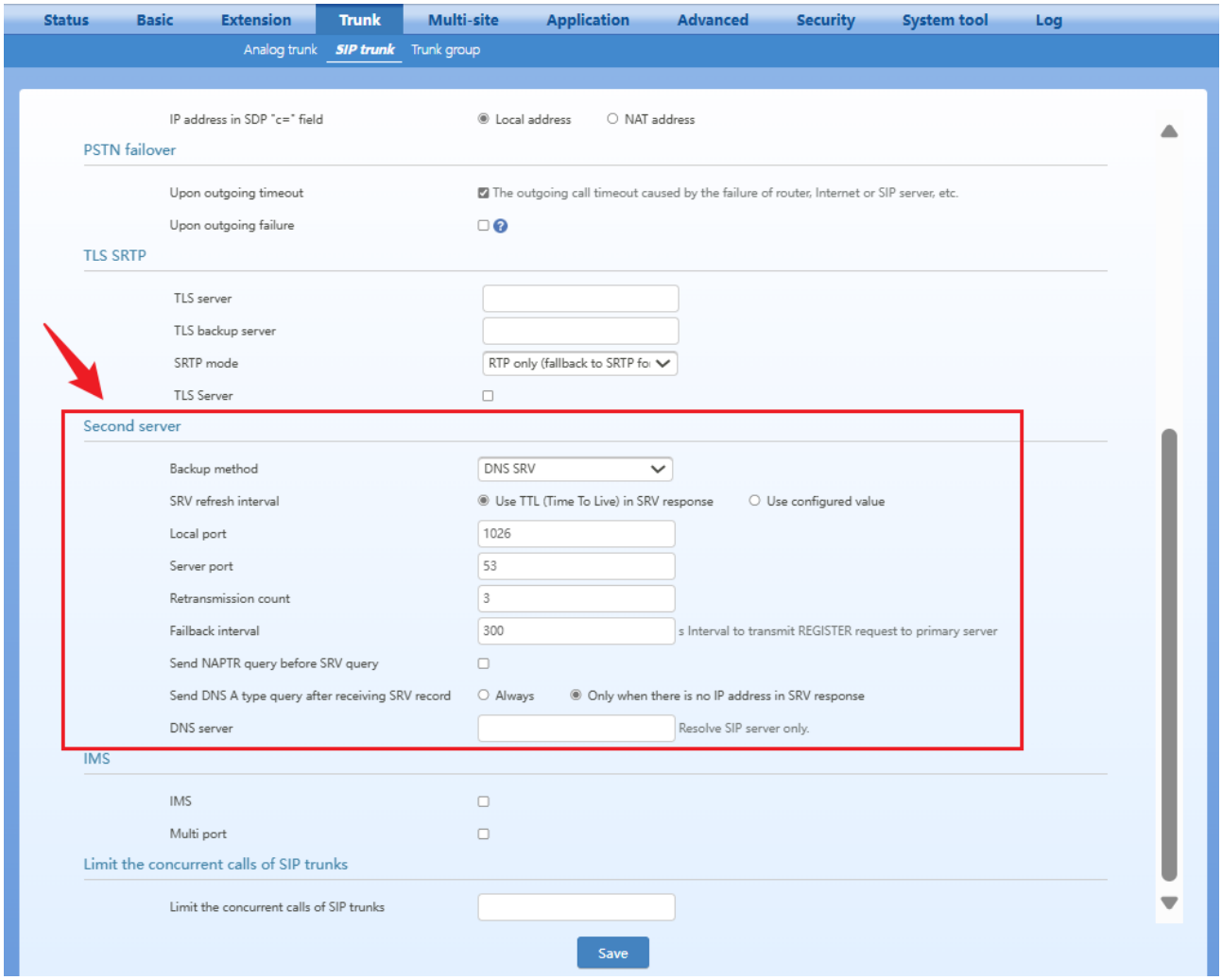


Table 2-12 Description of Backup Server Configuration Parameters

Parameters	Definition
Backup methods	• 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. If you choose the fixed mode, you need to set the backup server address provided by the VoIP operator, and you can check the "Main server status monitoring" option and set the OPTION request sending period (range from 2 to 65535 seconds) to monitor the main server status periodically. • 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.
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.

 Copyright © Redstone Systems, Inc

Parameters	Definition
Retransmission count	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.
Failback 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.
Send the DNS an A type query after receiving the SRV record	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. This configuration is available only for REX20/REX50.

Step 2 Select the backup mode.

Step 3 Save the settings.

2.3.4 IMS

REX can interface with IMS (IP Multimedia Subsystem). When interfacing with the IMS system, you need to configure IMS-related information in addition to configuring account registration on the SIP Outbound page.

The steps for configuring IMS-related information are as follows:

Step 1 Click Trunk> SIP Trunk > Registration Optionsand find the IMS Configuration item.

Figure 2-19 IMS Configuration Interface

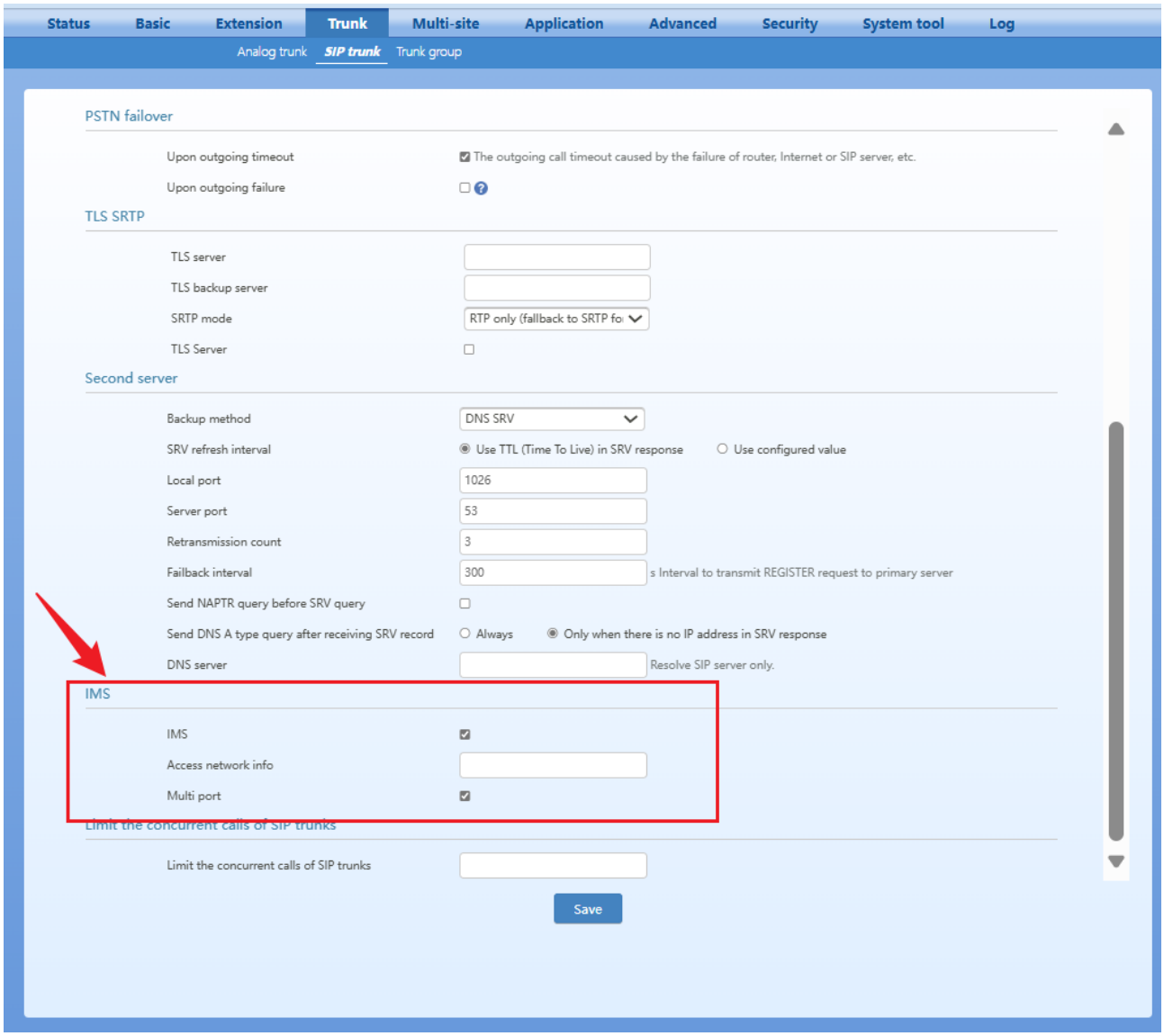


Table 2-13 Description of IMS interface parameters

Item	Definition
IMS	Check the box to turn on IMS.
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.
multiport	Open multi-port IMS docking.

Step 2 Check IMS and fill in the access network informationas required.

Step 3 Save the settings.

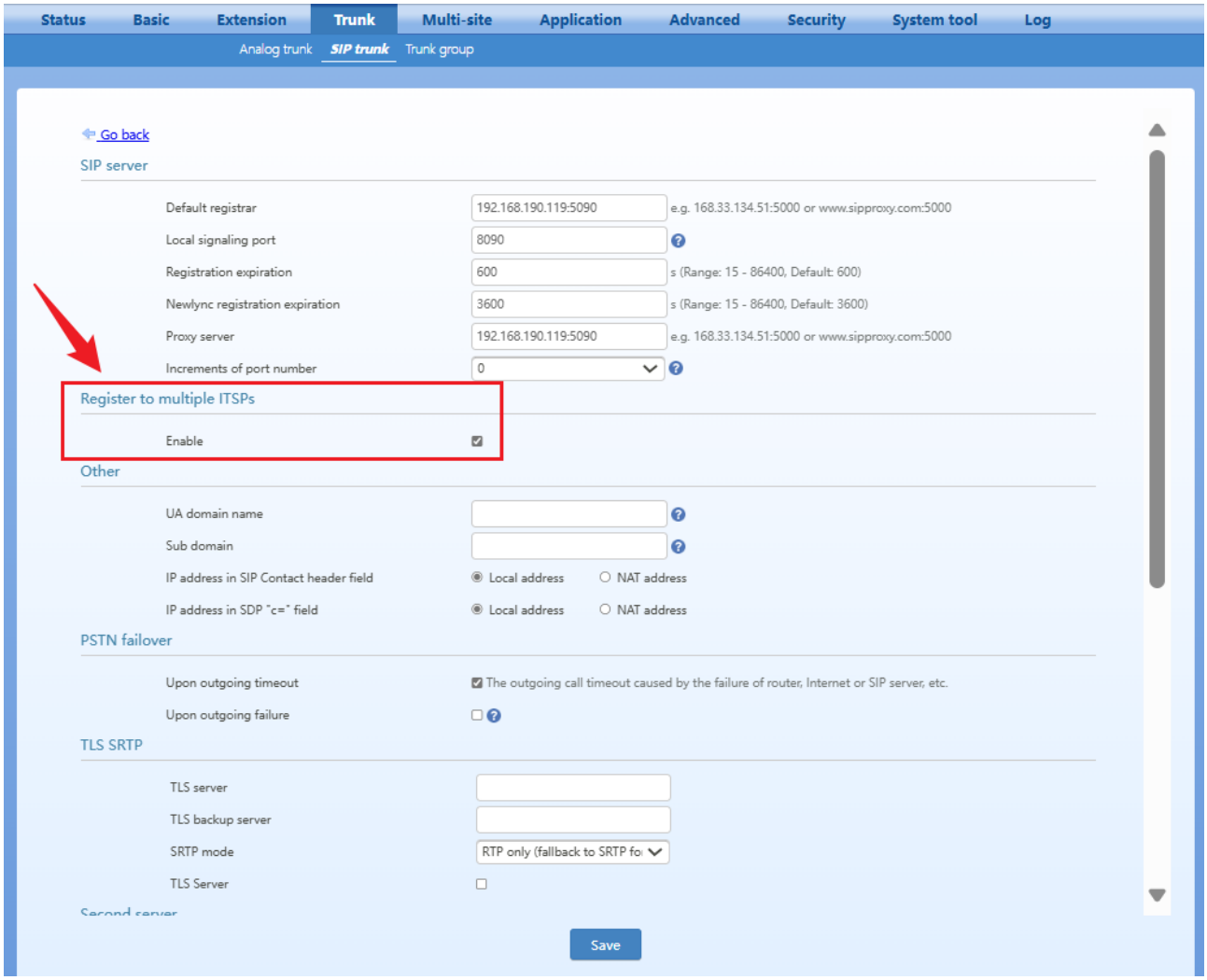
 Copyright © Redstone Systems, Inc

2.3.5 Directly Connected Trunk Groups

The user goes to Outside Line Settings > Direct Connect Trunk Groups, on this page the user can add or delete direct connect trunk groups.

Step 1 User goes to Outbound Settings > SIP Outbound, clicks the "Registration Options" button, and checks the box to allow "Registration for multiple platforms".

Figure 2-20 Register for the multi-platform configuration screen



Step 2 Go to Trunk>Direct Trunk Groups, click "Add" button to bring up the "Add Direct Trunk Group" page, users can fill in the parameters of the new direct trunk group.

 Copyright © Redstone Systems, Inc

Figure 2-21 Direct Connect Trunk Group Configuration Screen

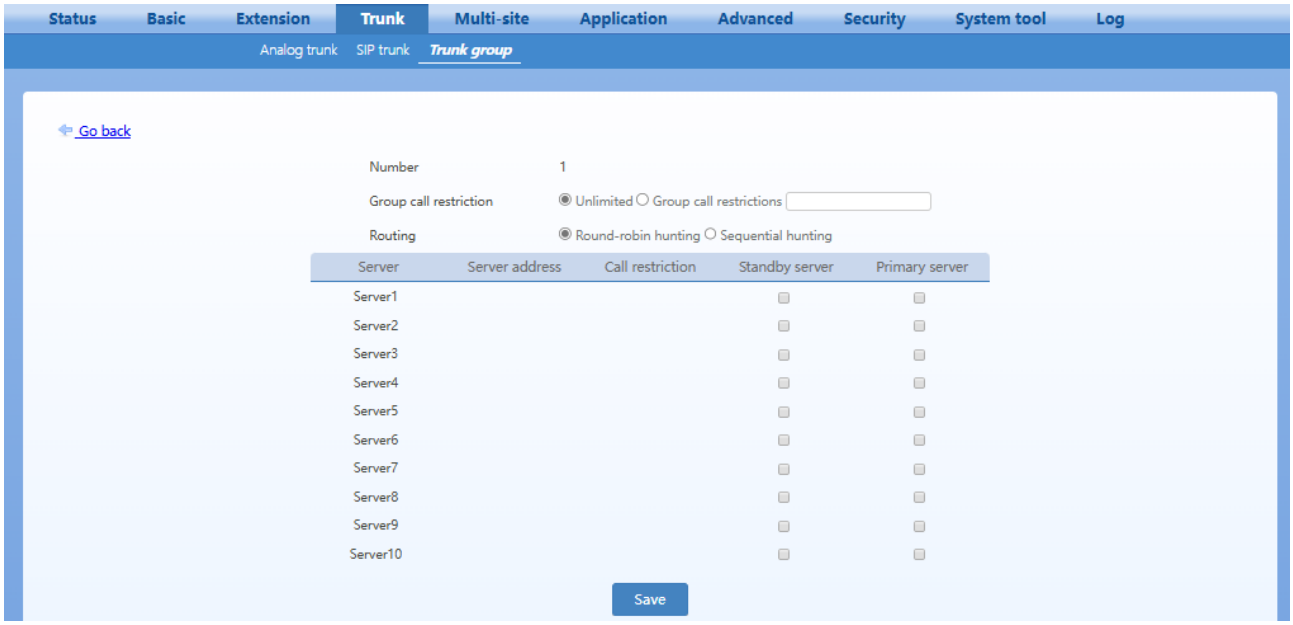


Table 2-14 Parameter description of the directly connected trunk group

Item	Definition
Batch number	The numbering of the added direct-connect trunk groups is numbered from #1 by
Group call restriction	The number of call concurrencies limited by a directly connected trunk group can be set to "Unlimited", or you can set the number of call restrictions for a directly connected trunk group (limited by the number of trunk concurrencies).
Selection method	When outgoing/incoming external SIP calls, the line selection method can be selected from "Circular" or "Shift Selection". Rotation: when there is a new inbound/outbound SIP outbound call, the call is equally distributed to each server in the order of 1, 2, 3; Shunted: when there is a new inbound/outbound SIP outbound call, Server 2 is enabled after Server 1 call occupancy; Note: If the primary server rotation is full, then switch the backup server, the backup server rotation is full, beyond the call failure (switching conditions are: reach the call qualifying number, invite no response, receive error code 5xx, such as 506, 503, when invite no response or receive 5xx code, the system will Retry 3 times, if it fails again, then the call will end).

Note:1. Up to 10 SIP TRUNK servers can be set up for a single directly connected trunk group. You can set the server IP address and set the number of call restrictions for individual servers on the page and set a server as the primary or backup server as required.

2.SIP calls are only supported in peer-to-peer mode.

3.If you need to modify the parameters of an existing directly connected trunk group, select the directly connected trunk group that needs to be modified and click the Edit button on the far right.

 Copyright © Redstone Systems, Inc

2.3.6 DID/DOD (REX1000)

DID means that after binding an outside number to an extension number, when a caller dials that outside number, the device bypasses the welcome message and delivers the call directly to the bound extension.

DID/DOD means that after binding the outside line number to the extension number, both inbound and outbound calls are one-to-one correspondence: when the caller dials the outside line number, the device bypasses the welcome message and delivers the call directly to the bound extension, and this outside line can only be used by the extension with which it is bound.

Step 1 Click Trunk > DID/DOD.

Figure 2-22 Linear (DID/DOD) Configuration Screen

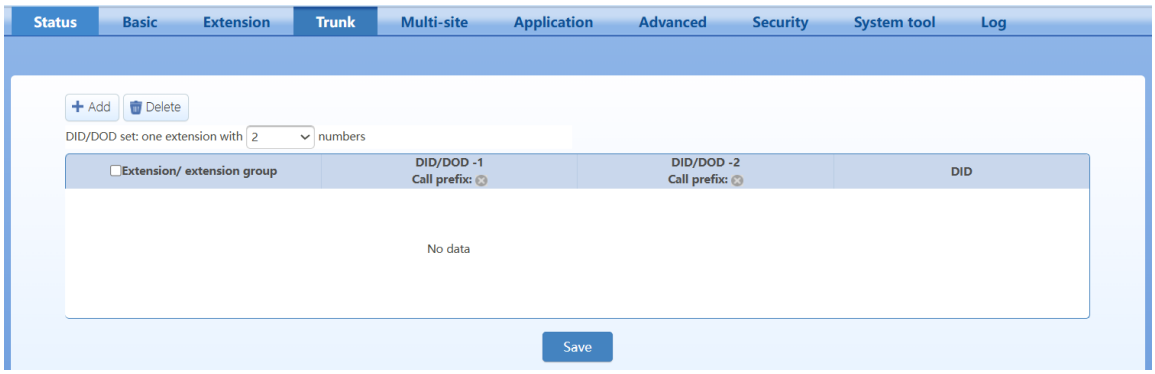


Table 2-15 Linear (DID/DOD) Parameter Description

Item	Definition
Add	Used to add DID/DOD rules.
DId/DOD set	Used to configure the number of DID/DOD outside lines corresponding to an extension/extension group, currently supports one extension/extension group can correspond to 4 outside lines.
Extension/extension group	Fill in the extension or extension group number that needs to be configured with DID/DOD function.

 Copyright © Redstone Systems, Inc

Item	Definition
DID/DOD	Fill in the outside line number. ● Inbound: The REX automatically delivers incoming calls from the outside number specified here to the corresponding extension or group of extensions. ● Outbound: when the filled extension/extension group calls out, the filled outbound resource is used. Note: You must set the outgoing prefix and the corresponding outgoing line number in the Basic Settings>Dialing Rules page, and you need to select Private Line for the outgoing mode. Then this prefix can only be given to the corresponding extension/extension group for outgoing calls. Other extensions/extension groups are not allowed to call out over this outside line.
DID	Fill in the outside line number. ● Inbound: The REX automatically delivers incoming calls from the outside number specified here to the corresponding extension or group of extensions. ● This outside line allows all extensions/extension groups to be used for outgoing calls.

Step 2 Save the settings.

2.4 Extension

REX supports analog extensions and IP extensions, which are described separately below.

2.4.1 Analog Extension (REX1000 does not have analog extensions)

Each FXS port corresponds to an analog extension number. the analog extension configuration procedure is as follows:

Step 1 Go to Extension Settings>Analog Extensions to manage the configuration of analog extensions.

Figure 2-23 Analog Extension Configuration Interface

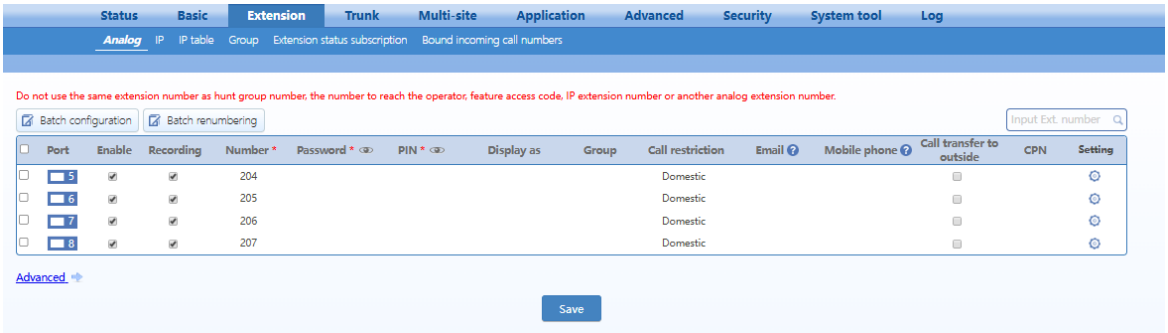


Table 2-16 Analog Extension Configuration Parameters Description

Item	Definition
Batch configuration	Batch configuration of extension functions.
Batch renumbering	Batch modification of extension numbers.
Port	Corresponds to the analog extension port (FXS port) on the device.
Enable	If this item is not checked, the line is not available. Enabled by default.
Number	The number of the analog extension that corresponds to the FXS port on the REX. The default is to start assigning numbers from 200. Note: All extension numbers cannot be duplicated, nor can extension numbers be duplicated with outside numbers.
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 unit. 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.
Display as	Configure the Display Name of the extension (analog extension and IP extension), which supports Chinese and English. Displaying names only applies to extension interdialing and requires the IP extension to support name display. If both the REX and the IP phone terminal are configured with a display name, the name configured on the REX takes precedence.
Group	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. For more information, please refer to 02.5.6 Group Substitution.
Call restriction	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.
Email	Enter the e-mail address to which the message file will be sent as an e-mail attachment if the extension has a voice message. For message related settings, please refer to 02.6.2 Messages.

 Copyright © Redstone Systems, Inc

Item	Definition
Mobile phone	After entering a cell phone number, you do not need to enter a password for verification when using the *33 and *99 functions when calling into the device with that number. If you also check the Direct dialing (Dial *33 Outbound) feature, after dialing the device's external number from this phone, you can directly use the device's resources to make an external call without entering *33.
Call transfer to outside	Check this item 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 function of transferring to an outside line, the extension must also have the corresponding outgoing call authority. Note 2: When transferring an outside call to an outside third party, you will be taking up two outside lines and incurring outgoing call charges. Administrators need to be cautious when turning on this feature.
Cpn	The extension's caller ID can be customized.
Setting	A variety of extension features can be configured: phone lock, call authorization, indentation dialing, same vibration number, black list, secretary phone, prohibit being answered on behalf of the caller, call waiting, do not disturb, call hold, call forwarding, transferring to an outside line, and so on. For details, see 02.5.1 Basic Functions.
Advanced	Advanced parameters for analog extensions can be set.

Step 2 Save the settings.

Step 3 Click Advanced to customize the advanced properties of the phone, such as gain, line impedance, etc. In general, if the extension is used normally, there is no need to modify the factory default parameters.

 Copyright © Redstone Systems, Inc

Figure 2-24 Analog Extension Advanced Settings Screen

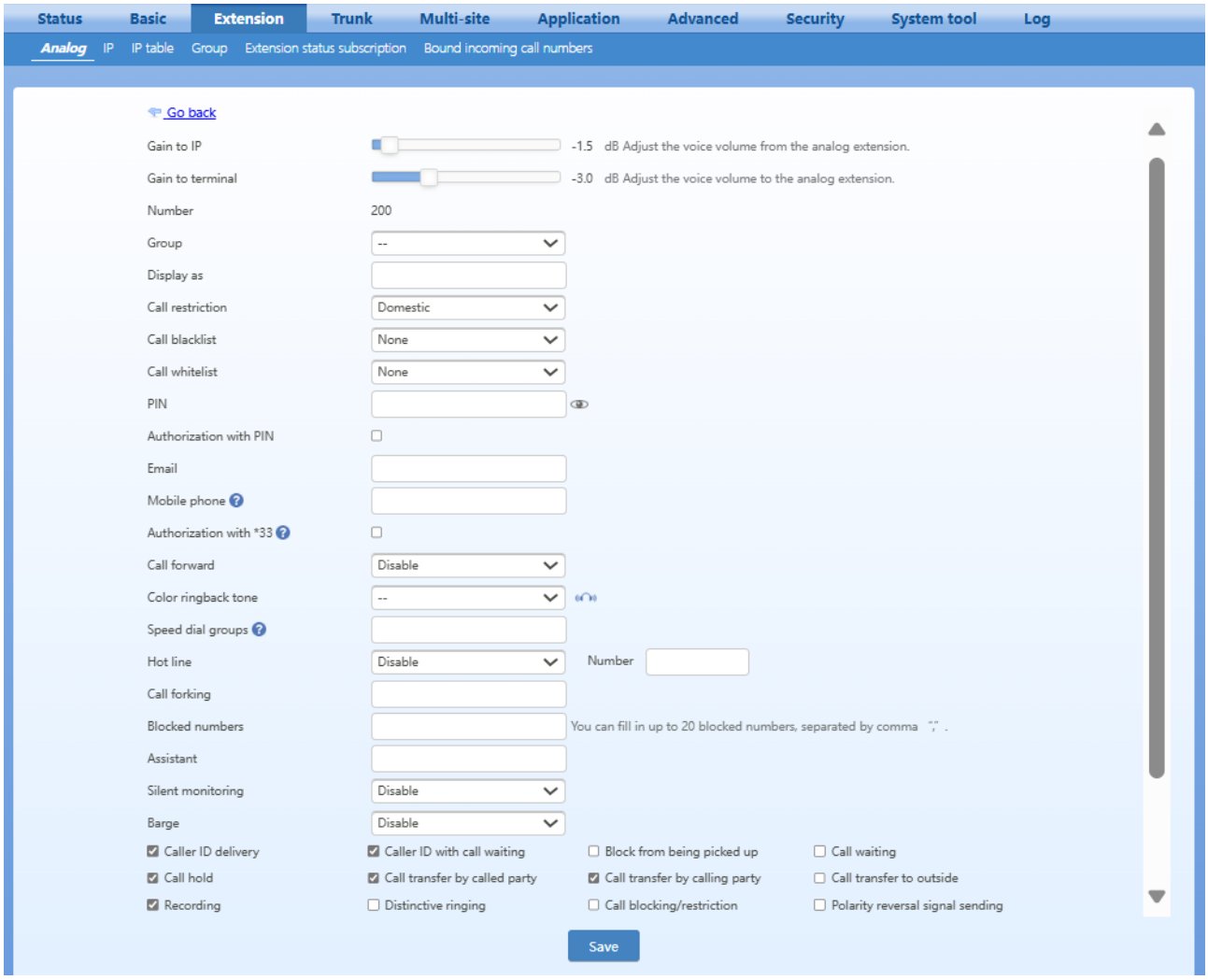


Table 2-17 Analog Extension Advanced Setup Parameter Description

Item	Definition
Gain to IP	Used to adjust the volume level received on the FXS port. When talking to an analog outside party, if the analog outside/IP outside/IP extension party's answer volume is too low or too high, the value of this parameter can be adjusted up or down. Range: -3.0 to +9.0 dB.
Gain to terminal	Used to adjust the volume level sent by the device to the FXS port line. When talking to an analog outside line/IP outside line/IP extension, this parameter can be turned up or down if the volume of the analog extension is too low or too high. Range: -6.0 to +3.0 dB.
Impedance	Selects the FXS port impedance. Includes composite, 600 ohm, and 900 ohm. Defaults to composite.

 Copyright © Redstone Systems, Inc

Item	Definition
Hook flash time min	Used to detect phone flash-off events, the default value is 75 milliseconds. The device will ignore flash-off events shorter than the minimum flash-off time. Normally, this value must not be less than 75 milliseconds. This parameter needs to be adjusted when the analog phone has the phenomenon of "ringing again after hanging up, but no voice when taking off the phone".
Hook flash time max	Used to detect phone flash-off events, default value is 800 milliseconds. The device will judge the flash breaks whose duration is between the shortest flash break and the longest flash break as valid flash breaks; the flash breaks which are greater than the maximum flash break duration will be judged by the gateway as hanging up and then taking off again. Typically, this value must not be less than 800 milliseconds.
Hook debouncing timer	Used to prevent the device from determining jitter in the state of the handset as being off-hook or on-hook. When the phone changes from the on-hook state to the off-hook state or from the off-hook state to the on-hook state, if the state duration is shorter than this value, the device ignores this state change and considers the phone is still in the original state. The value range is 10~1000, the default is 150 in milliseconds.
Ringing frequency	The default is 25 Hz, 1 second on 4 seconds off. No modifications are generally required. The range of values is 15 to 50 Hz.
Caller ID transmission mode	Generally, no modification is required. try adjusting this configuration when the caller ID is abnormal.
Hotline dialing relay	The delay time for the device to automatically dial out the pre-set hotline number after taking off the phone, the default value is 5 seconds, and the valid setting range is 2 ~ 20 seconds. Use when the "Hot Line" function is in "Delay" mode. See also Table 2-19.

2.4.2 IP extension

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

To use IP extensions, you need to configure the extension account and registration password on the REX first, and the configuration steps are as follows:

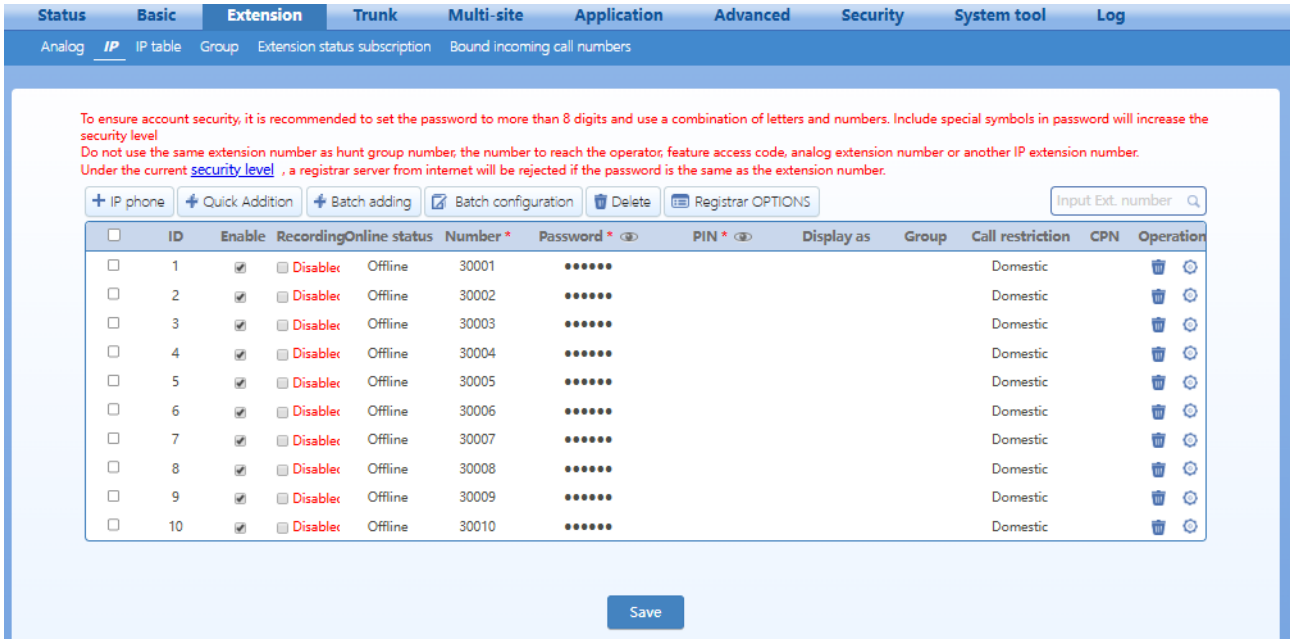
Step 1 Click Extension Settings > IP.

Step 2 Click Add, enter the extension account number and registration password, such as account number 208 and password187986.

Note: The REX20/REX50 has all IP extensions enabled by default.

 Copyright © Redstone Systems, Inc

Figure 2-25 IP Extension Account Configuration Screen



Note: The interface parameters are the same as Analog Extension (REX1000 does not have analog extensions) basic consistency.

Table 2-18 IP Extension Configuration Parameter Description

Item	Definition
Enable	If this item is not checked, the current line is not available. Enabled by default.
Online status	Displays the current online status of the extension.
Numbers	Extension number. Note: All extension numbers cannot be duplicated, nor can extension numbers be duplicated with outside numbers.
Password	The password used for extension registration. The factory default is the same as the PIN, but changing the password does not link to changing the PIN.
PIN, Group, display as, Call restriction, Settings	See also Table 2-16. Note: The default outgoing privilege for IP extensions is internal, and you can change the outgoing privilege only after you change the PIN code and password.

Step 3 Save the settings.

Detailed steps for registering an IP phone or softphone to the REX can be found in Appendix A IP Extension Registration to Device.

 Copyright © Redstone Systems, Inc

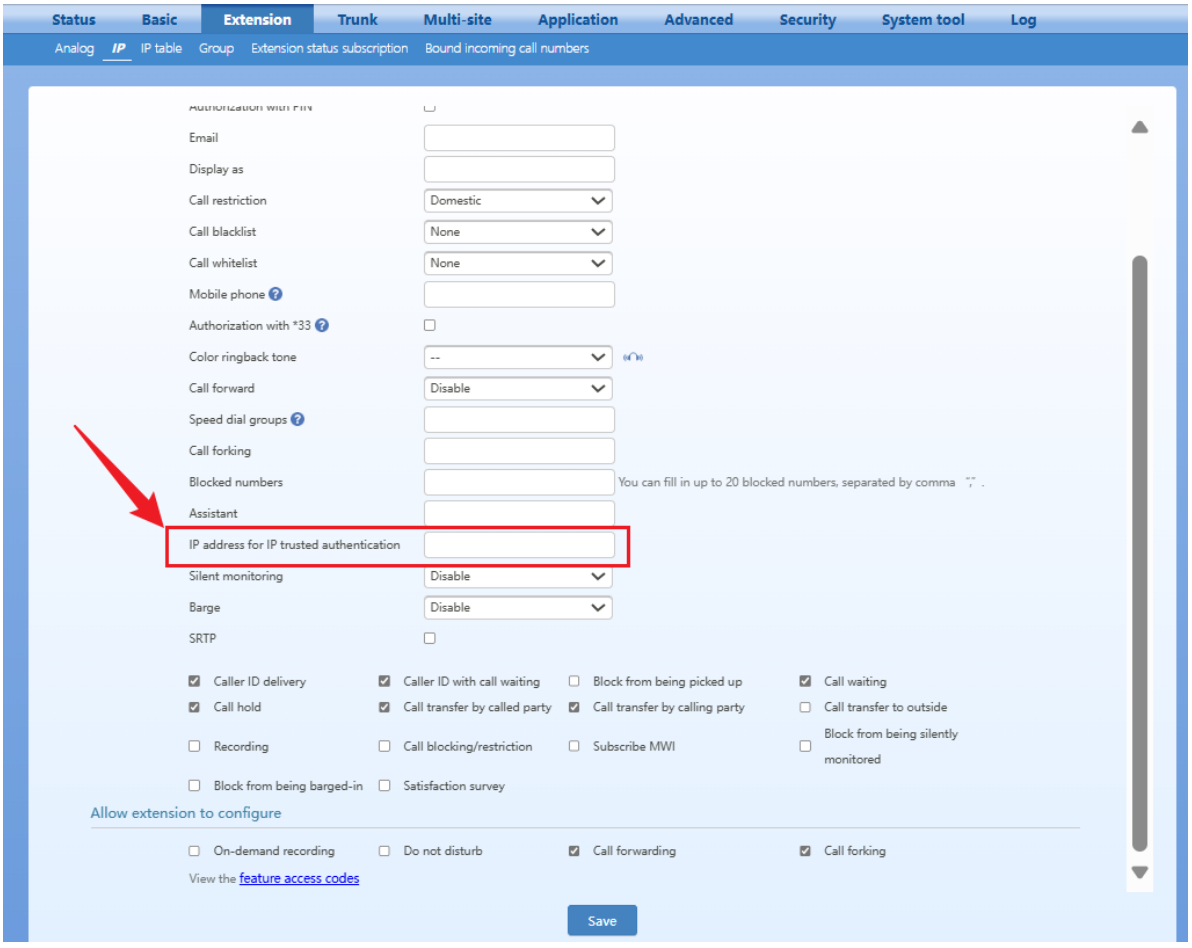
2.4.3 IP extension address authentication

When the REX and the IP address of an extension are reachable in both directions, after the address of the IP extension is entered into the REX, the REX will recognize the SIP end point from that address as a trusted endpoint, so that the IP extension can establish a SIP session with the REX without registration. This function is recommended when the REX is used with a companion gateway (e.g., MX60).

Go to Extension Settings > IP Extension, click Settings, and fill in the IP address of the terminal device when using IP address authentication, such as the IP address of the MX80E gateway used with REX.

Note: You also need to fill in the IP address of the REX at the proxy server on the gateway used in conjunction with the REX and set the subscriber line number to the extension number configured on the REX. Please refer to the MX User's Manual for detailed configuration methods.

Figure 2-26 IP Authentication Configuration Interface



 Copyright © Redstone Systems, Inc

2.4.4 One Number Supports Ten Devices

By registering IP extensions, it makes it possible to register and bind up to ten devices (i.e., ten machines) to one phone number (i.e., number one) at the same time. Enhanced number flexibility and interconnectivity between devices, suitable for application scenarios requiring multi-terminal access. The same number can be used on multiple devices at the same time, which facilitates flexible switching between multiple work terminals and improves call and management convenience.

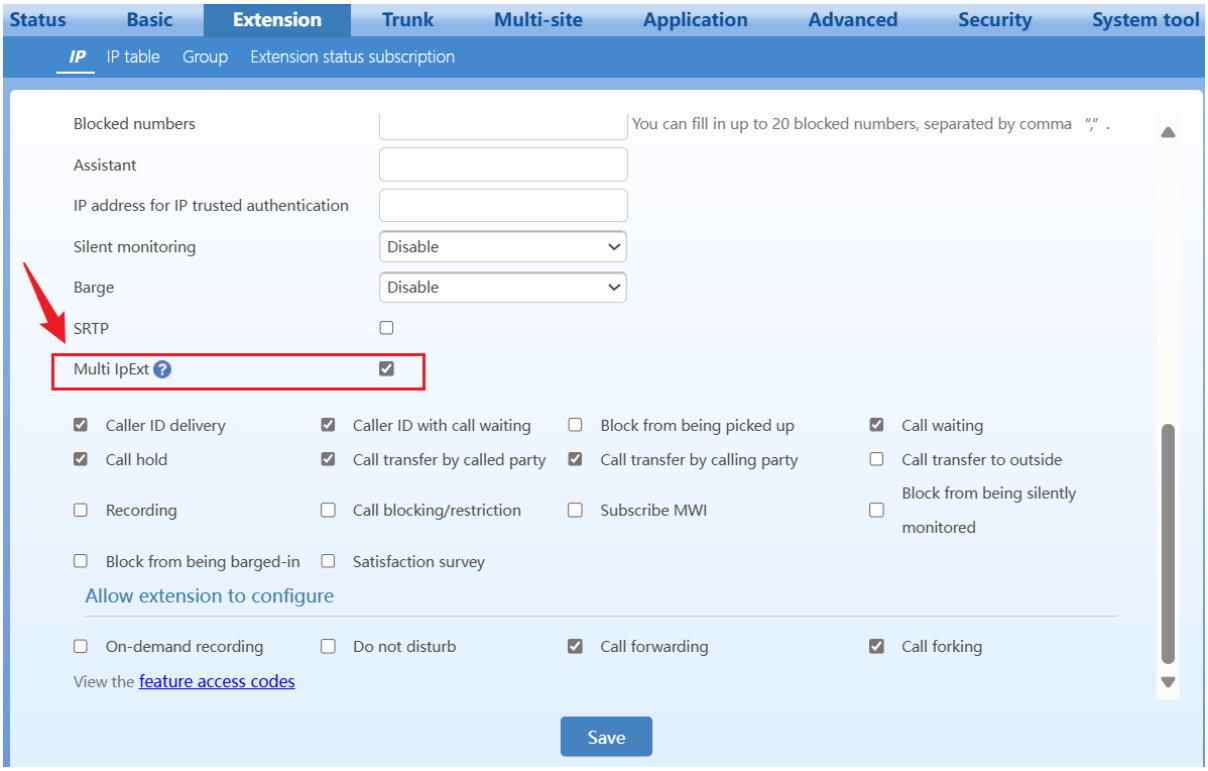
Step 1 Click on Hierarchy Settings > IP Extension

Step 2 Click the button

Step 3 Click to check the box to turn on the One Multi-Camera button feature

Step 4 Save Settings

Figure 2-27 One Number Supports Ten Devices Setting Interface



After the configuration is complete, you can check the number binding status on the Status Bar > IP Extension page.

 Copyright © Redstone Systems, Inc

2.5 Extension Functions

2.5.1 Basic Functions

Click Extension Settings>Analog Extension/IP Extension>Settings to set up the basic functions of the extension.

Figure 2-28 Extension Function Configuration Interface

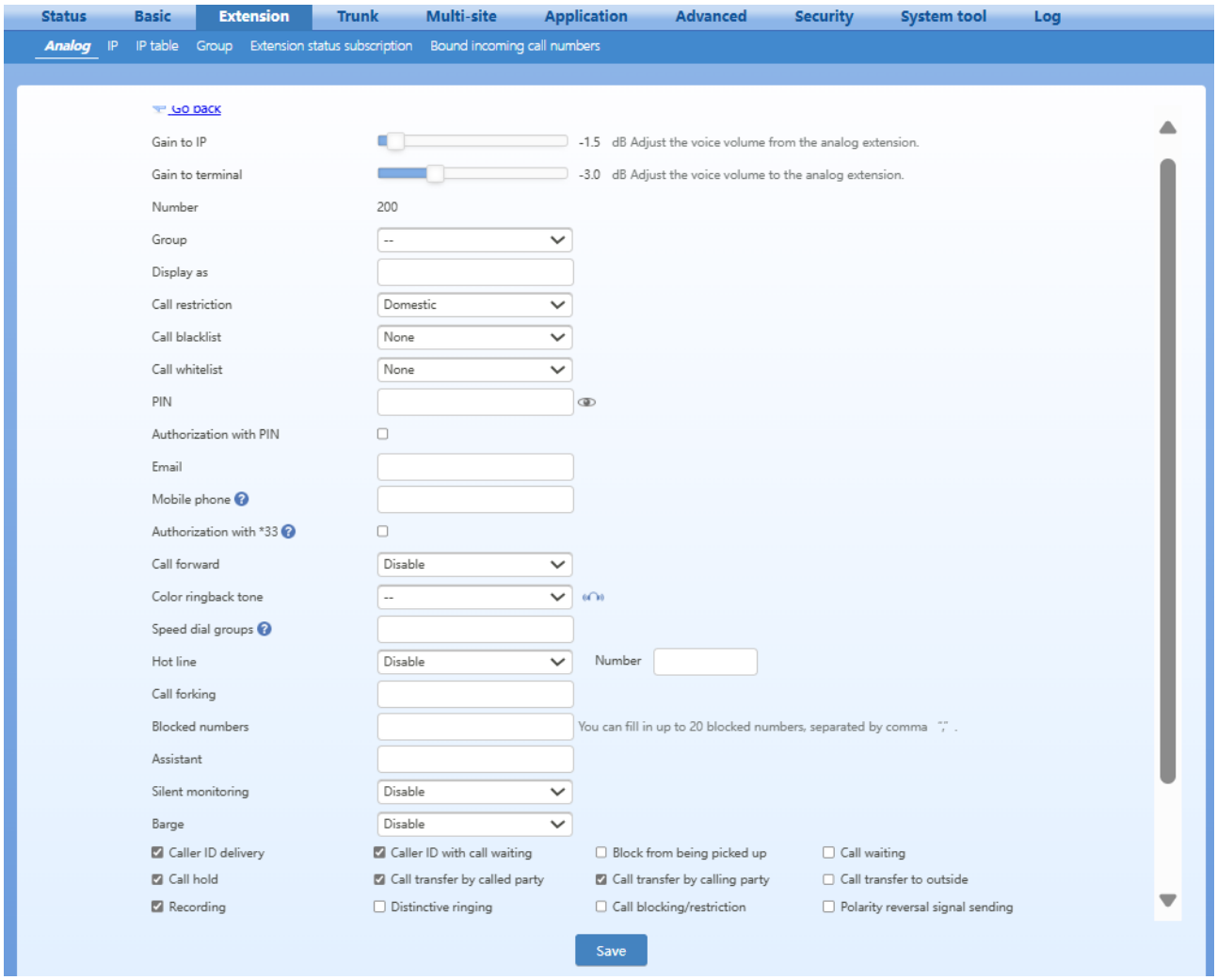


Table 2-19 Extension Basic Functions

Item	Definition
Gain to IP	Used to adjust the volume level received on the FXS port. When talking to an analog outside party, if the analog outside/IP outside/IP extension party's answer volume is too low or too high, the value of this parameter can be adjusted up or down. Range: -3.0 to +9.0 dB.
Gain to terminal	Used to adjust the volume level sent by the device to the FXS port line. When talking to an analog outside line/IP outside line/IP extension, this parameter can

 Copyright © Redstone Systems, Inc

Item	Definition
	be turned up or down if the volume of the analog extension is too low or too high. Range: -6.0 to +3.0 dB.
Number	Extension number
Group	See Table 2-16.
Authorization code (pin)	See Table 2-16.
Extension lock	Check the box to lock. Locked extensions can only dial internal lines; calling external lines requires authorization code (PIN) authentication.
Inbox	See Table 2-16.
Display name	See Table 2-16.
Call-out authority	See Table 2-16.
Call blacklisting	Set up a blacklist of extensions for outgoing calls.
Call whitelisting	Set up a whitelist of extensions for outgoing calls.
Mobile telephone number	See Table 2-16.
Through Train(currently shown on the interface as dial *33 outbound)	The Straight-Through feature allows a preset cell phone (e.g., an employee's cell phone) to make an outbound call through the device without having to enter a feature code after calling into the device's outbound 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 devices 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 Codepage.
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 an extension to voicemail. For voice mail related settings, please refer to 02.6.2 Messages. • 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. Note: You can set the ringing time before no-answer transfer in Advanced Settings>System>Number of Rings to Trigger No-Answer Transfer.
Caller ring-back tone	Selection of color ringtones for extensions, uploading and management of color

 Copyright © Redstone Systems, Inc

Item	Definition
(CRBT)	ringtone files.
Indentation dialing group	Reduced-digit dialing allows users to replace actual numbers with pre-set two-digit numbers, providing a convenient, easy-to-remember dialing method. For example, using 20 as the abbreviated code for 13823218765, simply dial **20 when making a call. Reduced digit dialing group consists of "Reduced Digit Code - Phone Number" (e.g. 20-13823218765), the range of the reduced digit code is 20~49, and a maximum of 30 groups can be configured, each group is separated by ",".
Hotline	The device automatically calls the hotline number after 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 REX's web interface can only set up hotline functions for analog extensions. Hotline functions for IP extensions need to be set up on the IP phone.
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 REX's extension number or external number, etc. Notes: • When Do Not Disturb, Unconditional Call Forwarding, and Secretarial Extension are turned on, Simultaneous Oscillation does not take effect. • If an incoming call is on hold, co-oscillation does not take effect. • Co-oscillation to external terminals via an analog external line, which needs to support reverse polarity signals. If the external line does not provide a reverse polarity signal, the unit will ring the extension first, with a no answer timeout before sending the incoming call to the external terminal.
Rejected caller ID	Users can fill in the numbers they don't want to answer here and the device will play a busy tone alert to the caller. If you fill in more than one number, please separate them with ",". Note: Extensions can call numbers in this list normally.
Secretarial extension	By tying an extension to a secretarial extension, calls to that extension will be routed to the secretarial extension and answered by the secretary. You can go to Application Services>Secretary to check the secretarial method as needed: • 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.
Addresses when using	Set the IP address when using IP authentication (for IP extensions only).

 Copyright © Redstone Systems, Inc

Item	Definition
IP authentication	
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: Allows this extension to listen to the same department Allows this extension to listen to calls from any extension in the same department. Note: If one of the extensions on both sides of the ongoing call has Listening Mask enabled, listening will not take effect.
Force insertion	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.
SRTP(IP extensions only)	Check to enable the SRTP function.
Caller ID	With Caller ID turned on, when an outside line calls an extension on the REX, the calling number is displayed on the extension. Not turned on, then not displayed
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.
Prohibition of substitution	When an incoming call on an extension is not answered, other extensions can answer it on behalf of the extension. Turning on this function prohibits incoming calls to this extension from being answered on behalf of other extensions. Note: The function of 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.
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 extensionis 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

 Copyright © Redstone Systems, Inc

Item	Definition
	party displays the number of the intermediary transferor. Note: Before using the transfer function, make sure thatthe call 5 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: ibid. Note: Before using the Call Forwarding feature, make sure Call Hold, Call Forwarding is turned on.
Transfer to an external line	See Table 2-16
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 02.6.1 Recordings the specific settings of recording can be referred to.
Distinctive ringing (analog extensions only)	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 02.10.4 Call restriction.
Extension message subscription (IP extensions only)	When this function is turned on, subscribe to listen to messages on IP extensions.
Reverse polarity signaling (analog extensions only)	When the remote end answers, the device provides a polarity reversal signal to this terminal, and again when the remote end hangs up. Reverse polarity signals can be used on phones with billing.
Do not listen in	When this feature is turned on, calls from this extension will not be allowed to be listened to.
Prohibition of forced penetration	When this feature is turned on, calls from this extension are not allowed to be forcefully inserted.
Satisfaction survey	When checked, the satisfaction survey voice is automatically played at the end of the call.

 Copyright © Redstone Systems, Inc

2.5.2 Dialing an outside line

Click Basic Settings>Dialing Rules to configure outbound rules.

Figure 2-29 Outbound Rule Configuration Interface

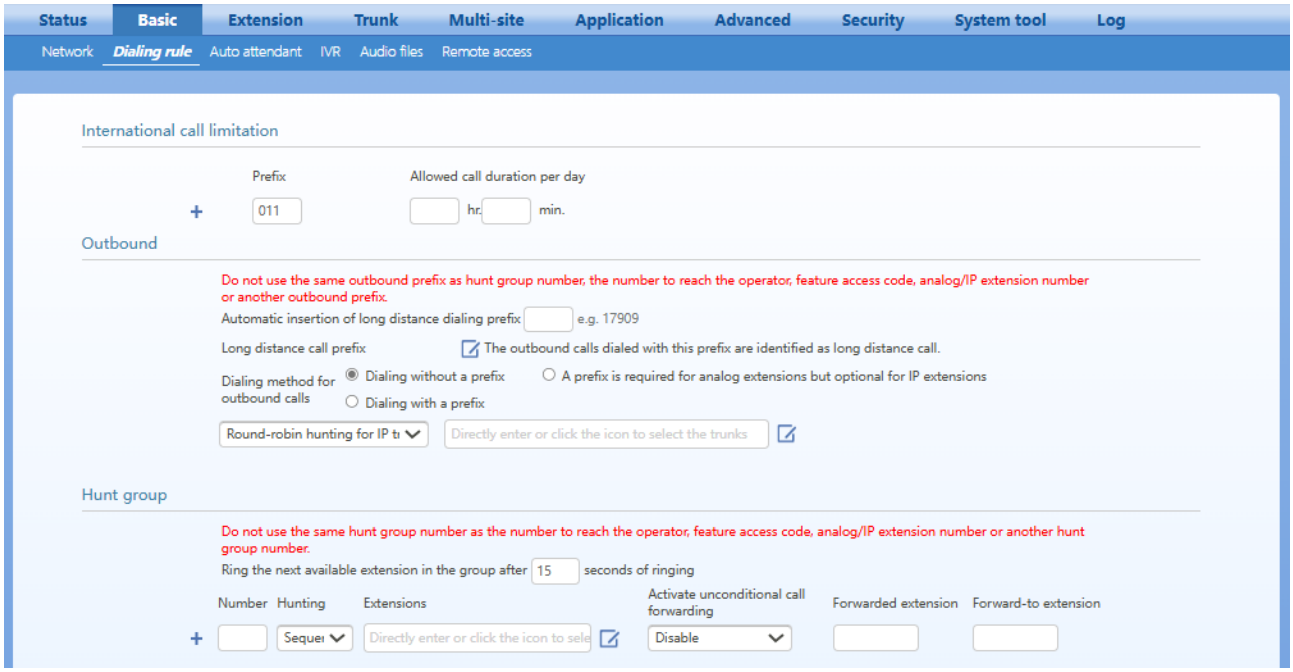


Table 2-20 Outbound call rule parameter description

Item	Definition
International call limitation	When an extension user dials an outgoing number, if the number starts with the number configured here, the device will automatically recognize this outgoing number as an international long-distance number and limit the daily outgoing call duration. The number header defaults to 00. Note: When the extension outgoing authority is Prohibited, Intercom, City or Domestic, you cannot call a number with an international prefix.
Automatic insertion of long distance dialing prefix	When an extension user makes a long-distance call through an analog outside line, the device will automatically add the number set here as a prefix.
Long distance call prefix	When an extension user dials an external number that begins with the number configured here, the device recognizes the external number as a domestic long-distance number. Numbers with domestic long-distance prefixes cannot be called when the extension's outgoing authority is Prohibited, Intercom, or City. Domestic long distance number header defaults to 0. The device supports recognizing the attribution of cell phone numbers in mainland China. If an extension dials a foreign cell phone without dialing 0, the device will automatically add 0 and then call out.

 Copyright © Redstone Systems, Inc

Item	Definition
Dialing method for outbound calls	• Direct dialing for both external and internal lines: Extension users can directly dial internal extension numbers and external numbers. • Outside line direct dialing, internal line plus dialing *: Extension users can directly dial the outside number, dialing the internal extension need to add *. • Add prefix to the external line and direct dialing to the internal line: extension users can direct dial the internal extension number, and add prefix to select the outgoing line when dialing the external number.
Selection method	When the device is configured with multiple outgoing lines, you can select the corresponding outgoing call routing method according to the actual need. The device provides the following six outbound call routing methods: • Analog Outside Line Sequential selection: By analog outside line outgoing, and according to the analog outside line number arrangement order set in the Outside Line Input box, the first free line outgoing is always selected. For example, the numbers filled in the Outbound field are 654321, 654322, 654323, currently 654321 is being used for outgoing calls, at this time another outgoing call will select 654322 for outgoing calls. • Analog Outside Line Circular: By analog outside line outgoing, and according to the analog outside line number arrangement order set in the Outside Line Input box, take turns to select the free line to call out. For example, the numbers filled in the Outgoing Line column are 654321, 654322, 654323, if the last call is outgoing through 654321, then another outgoing call will select 654322 to call out (when 654322 is idle), and if 654322 is busy, 654323 will be selected to call out. • SIP Outside Line Sequential: Outgoing via SIP outside line and always select the first free line to call out in the order of the SIP outside line number set in the Outside Line Input box. 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 and rotate to select the free line to call out according to the arrangement order of the SIP outside line number set in the outside line input box. 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, if there is another outgoing call, 754322 will be selected for outgoing call (when 754322 is idle), if 754322 is busy, 754323 will be selected for outgoing call. • Intelligent outbound: local calls are outbound via analog outbound, long-distance calls are outbound via SIP outbound. The device uses the domestic/international long distance number header to determine whether the dialed call is a long-distance call. For example, if the domestic long-distance prefix is 0 and the international long-distance prefix is 00, calls to numbers beginning with these two digits are outbound via a SIP outbound line, while local calls are outbound via an analog outbound line. When the SIP outside line is not available or a network failure occurs, it will be called out via an analog outside line. Note: When all SIP outside lines are occupied, you will hear a voice prompt when dialing long distance: there is currently no free outgoing line. ● Routing: using the routing table to set specific routing rules. Note: When the line selection method is down/round selection, the REX200/REX200-A/REX500 /REX1000 can set up to 60 outside line numbers for a prefix, and the REX50 can set up to 40 outside line numbers.

 Copyright © Redstone Systems, Inc

Item	Definition
Prefix	Users can select the corresponding line selection method when dialing an outgoing line by using the outgoing call selection prefix configured here. For example, if the outgoing line selection prefix is set to 9 and the corresponding line selection method is set to SIP outgoing line by-pass, the device selects SIP outgoing line and calls the other party by by-pass when the user dials 9 before making an outgoing call. Note 1: This parameter can be configured only when the outbound dialing method is Outbound Plus Dialing Prefix and Inbound Direct Dialing. 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.
Secondary 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 can be configured only when the outbound dialing method is Outbound plus dialing prefix and Inbound direct dialing.
Trunk	Set the outgoing trunk group, i.e., select each outgoing line number corresponding to the analog outgoing line/SIP outgoing line smooth selection and round selection. Outside numbers can be selected directly or entered manually, with each number separated by a half comma ",".

2.5.3 Inbound/outbound number filtering

Click Extension Settings>IP table 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.

Figure 2-30 Number Filtering Configuration Interface

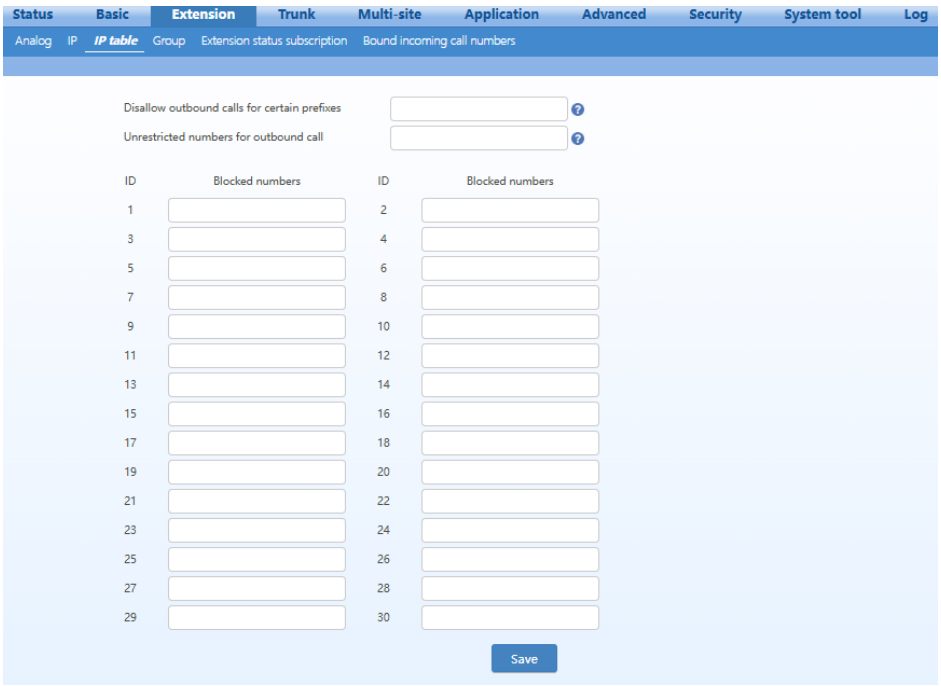


Table 2-21 Parameter Description of Number Filtering Interface

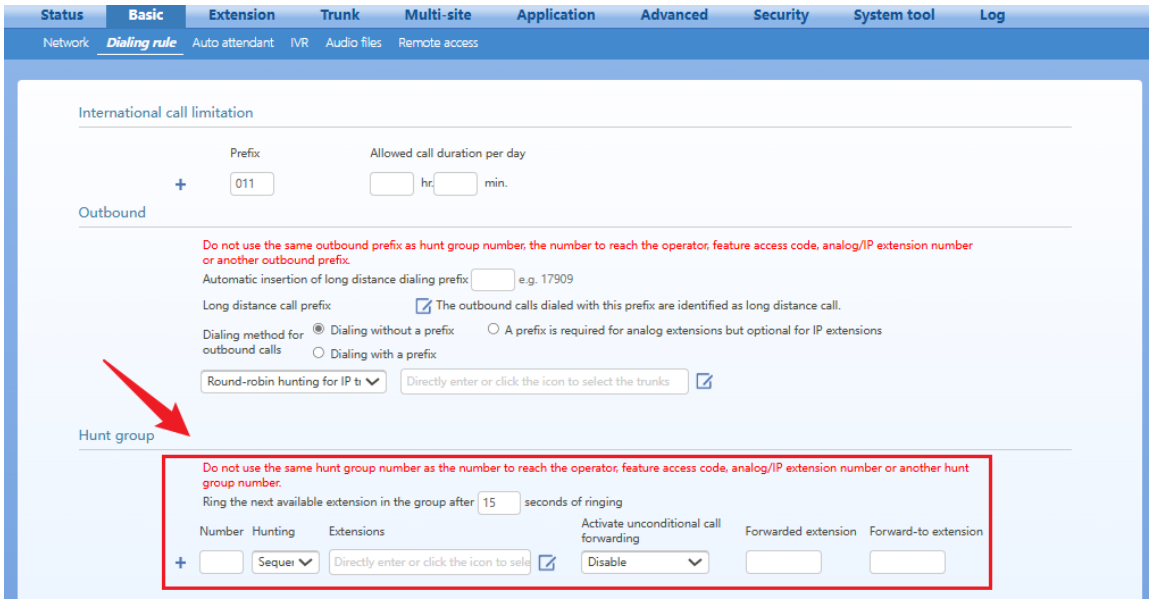
Item	Definition
Disallow outbound calls for certain prefixes	Extension users are prohibited from calling numbers with a prohibited outgoing call prefix, and the device will play a busy tone alert when an extension user dials these numbers. Up to 20 prefixes or numbers can be set, separated by half commas ",". Note: Numbers in the Unrestricted Outbound Numbersare not subject to this restriction.
Unrestricted numbers for outbound calls	Extension users dialing an unrestricted outbound number will not be subject to any restrictions, including outbound privileges and prohibited outbound prefixes.
Blocked numbers	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 rejected call number configured here applies to all extensions, while the rejected call number in the extension settings only applies to the corresponding extension. For more information, please refer to 02.5.1 Basic Functions.

2.5.4 Call answering team

Assign multiple extensions to an incoming call answering group. When the caller dials the group number, the device will ring the idle extensions in the group according to the pre-set assignment.

Click Basic > Dialing Rules to configure call answering groups, and click ➕ to add a new group.

Figure 2-31 Call Answer Group Configuration Interface



 Copyright © Redstone Systems, Inc

Table 2-22 Parameter description of the call answering group

Item	Definition
Ring the next available extension in the group after XX seconds of ringing	If the extension ringing duration exceeds the value set here when the assignment method of the extension group is Circular or smooth selection, the next extension is rung.
Batch number	The number of the call answering group. Note: Please avoid conflicts with outgoing call prefixes, transferring switchboard numbers, extension numbers, feature codes, etc.
Mode of distribution	When there is more than one extension in the call answering group, you can select the corresponding distribution method according to the actual need. The device provides the following 3 types of distribution: • Sequential: Always select the first available extension to answer an incoming call in the order of the extension numbers set in the Group Extension Numbersbox. For example, the numbers filled in the group extension are 221, 222, and 223, if 221 is currently on a call, the incoming call will select 222 to ring. • Circular: Take turns selecting an idle extension to answer an incoming call in the order in which the extension numbers set in the Extension Number box of the groupare listed. For example, the number filled in the group extension is 221, 222, 223, the last extension that answered the incoming call is 221, at this time there is an incoming call will first select 222 ringing (when 222 is idle), if 222 is busy line, it will select 223 ringing. • Simultaneous: all free extensions in the group ring at the same time, the first one to pick up the call. A maximum of 60 extensions are allowed to be set up in REX200/REX200-A/REX500/ REX1000 group oscillator groups, and a maximum of 40 extensions are allowed to be set up in REX20/REX50 group oscillator groups. Attention: • If the distribution method is Sequential or Circular, and Call Forwarding is set for an extension in the group, the device will transfer the incoming call to the target extension when ringing to this extension, and the incoming call will not be forwarded back to the other extensions in the group if no one is available at that extension to answer the call. • Support extension group call queuing function, queuing for incoming calls will hear the voice prompt "extension is busy, please wait patiently". Note: A maximum of 20 incoming calls will be allowed to queue.
Extension number within a group	Fill in the extension number within the call answering group.

 Copyright © Redstone Systems, Inc

2.5.5 Extension Status Subscription (REX20/REX50/REX1000)

On the Web interface of the device, you can subscribe to the call status of other extensions for the supporting NRP1004 and NRP1012 models. After successful subscription, the current status of the subscribed extension can be indicated by the function key indicator on the phone. The extension subscription indicator corresponds to the extension status as shown in the following table:

Table 2-23 Extension Subscription Indicator Status Description Table

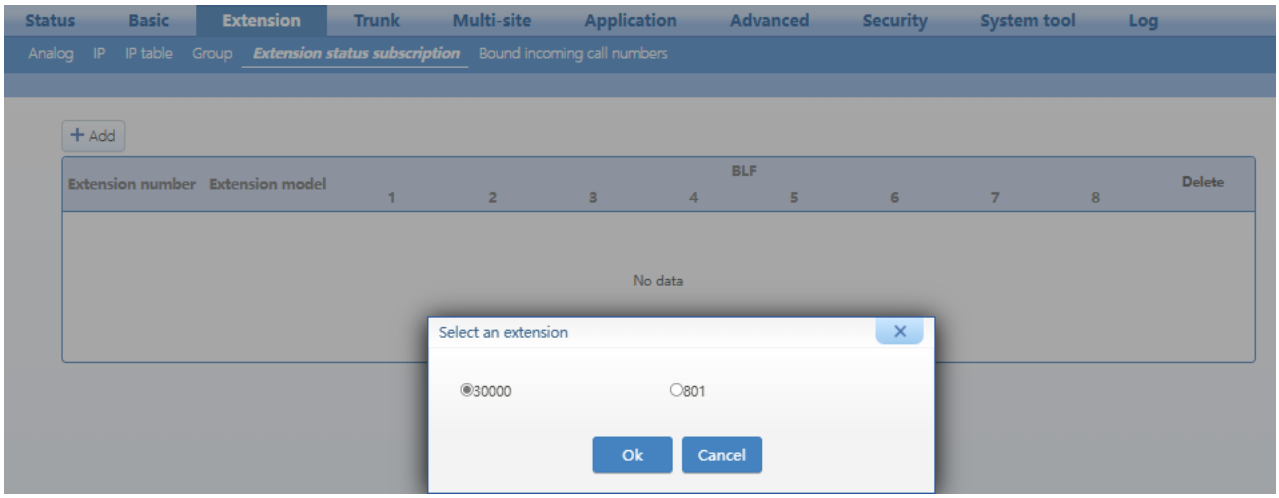
Extension status	Indicator status
Leisure time	lit. the green light stays on forever
Bell ringer	red light flashing
During a conversation	lit. the red light stays on forever
Extension not online	lit. the red light stays on forever

The configuration steps are as follows:

Step 1 Go to Extension >Extension Status Subscription and click Add to add status subscription information.

Step 2 Select the extension for which subscription information is configured.

Figure 2-32 Extension Status Subscription Screen



Step 3 Select the model of the current extension.

Select the model that matches the actual phone, otherwise the function key configuration will not take effect. The NRP1004 and NRP1012 have 4 and 8 LED

 Copyright © Redstone Systems, Inc

keys, respectively, which can be used to display the status of other extensions.

Figure 2-33 Selecting an Extension Model



Step 4 Select the extension number to which you want to subscribe from the drop-down list of function keys.

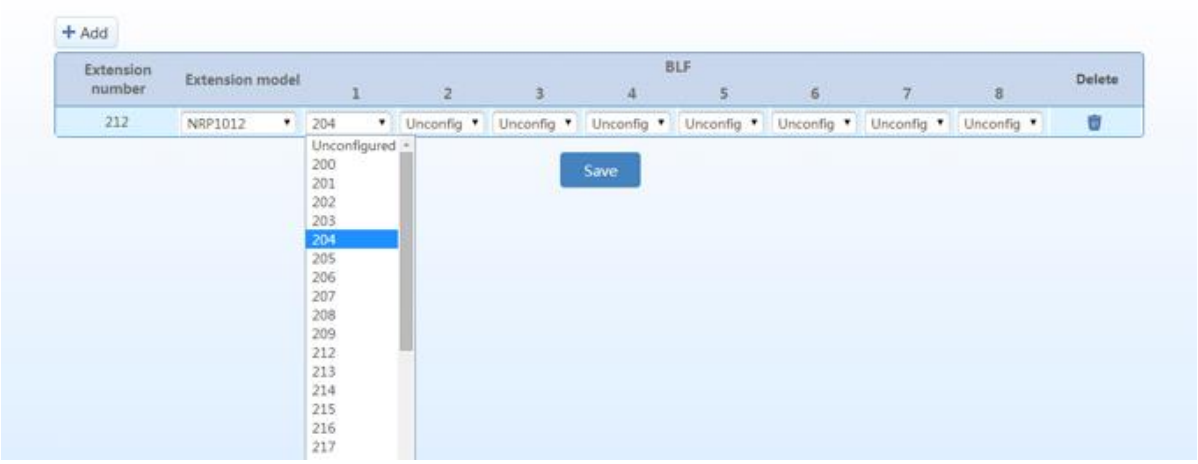
Figure 2-34 Subscription Extension



Step 5 Save the settings.

After the configuration is complete, you can view, change, or delete the subscription information for the current extension on the Extension Status Subscription page of the device.

Figure 2-35 Extension Status Subscription Main Screen



When the phone's subscription cycle arrives or after rebooting the phone, the phone will automatically download the subscription configuration from the device. If the phone has not yet been registered as an extension of REX, connect the phone to the device and power it up, then fill in the authorization code of the corresponding extension in the PIN code input box. When the download is complete and the phone reboots, the phone's function key indicator lights up.

Note

If the group vibration group has no more than 5 extension members, the extension state in the group supports being subscribed.

2.5.6 Group Substitution

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.

Configure the steps of the department:

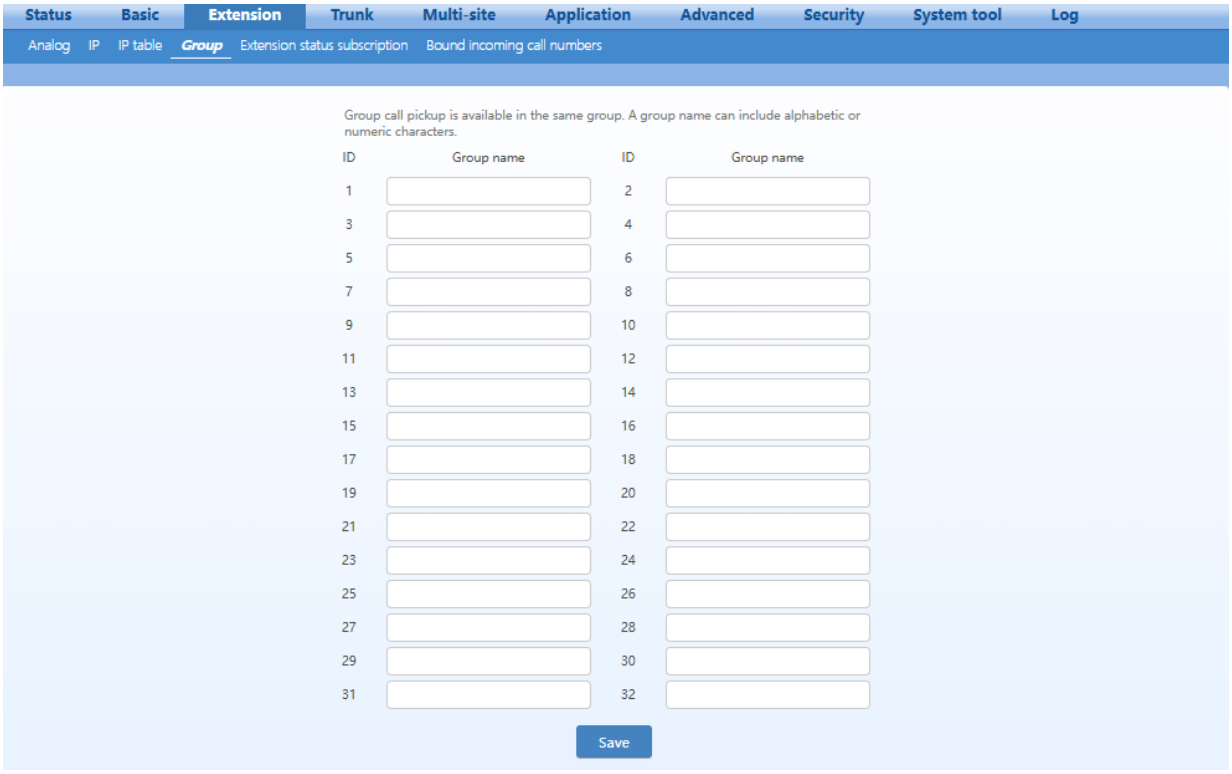
Step 1 Click Extension >Group to enter the Department Settings screen and fill in or change the department name.

Up to 32 departments can be set up.

Step 2 Click Save.

 Copyright © Redstone Systems, Inc

Figure 2-36 Department Configuration Screen

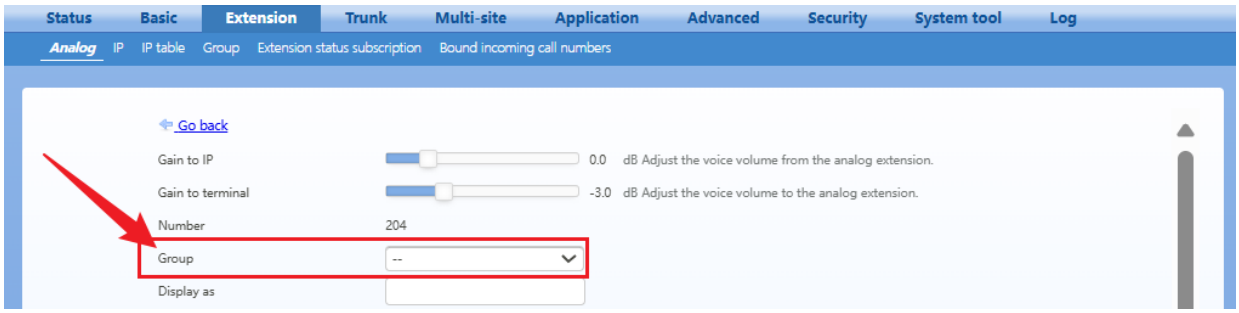


Steps for dividing extensions into specific departments:

Step 3 Go to Extension Settings>Analog Extension/IP Extensionand click the Setup button to enter the Extension Function Configuration screen.

Step 4 Select the department to which the current extension is categorized in the Department drop-down list to save the settings.

Figure 2-37 Extension Department Selection Screen



2.5.7 Substitute connection

When an extension call goes unanswered, another extension user can answer the call on behalf of the extension user. The Extension Substitution function is enabled by default

 Copyright © Redstone Systems, Inc

and can be operated directly on the phone without setting on the device.

2.5.8 Three-way calling

Extension users can invite a third party to join them during a call to realize a three-way call, or talk to one party while the other party listens to background music and waits, and can switch between call recipients at any time. Either other party can voluntarily exit the three-way call by hanging up without affecting the call with the other party, or can end the three-way call at any time by hanging up.

Note: With Call Hold on, three-way calling is enabled by default and can be operated directly on the phone without setting it on the device. For call hold related settings, please refer to Call Hold for call hold related settings.

2.5.9 Call Parking

An extension user can temporarily put the current call on hold and hang up during a call, at which time the device will play background music to the other party, and then the extension user can continue to talk to the other party at other extensions in the system.

Note: With Call Hold on, Call Parking is on by default and can be operated directly on the phone without setting it on the device. For details on settings related to call hold, please refer to Call Hold for details on call hold related settings.

2.5.10 DID

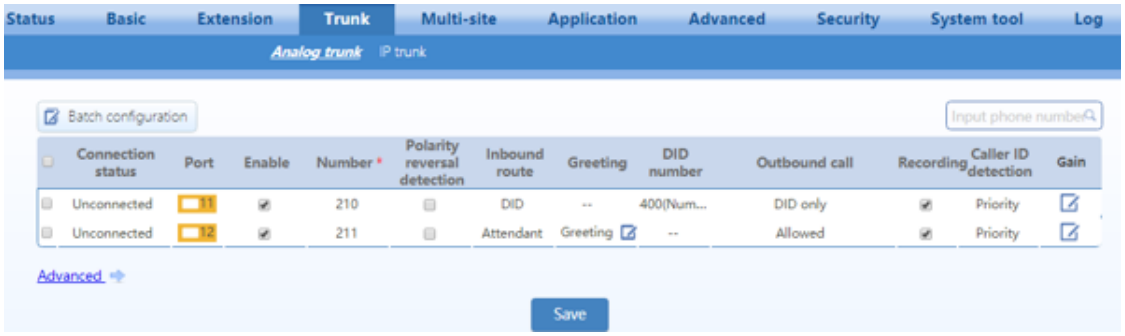
Outside lines can be tied to extensions/call answering groups. When an incoming call comes in, the unit will bypass the automated switchboard and deliver the call directly to the tied extension/call answering group. Bound outside lines can be set to be dedicated to the corresponding extension/call answering group, or can be set to be shared with other extensions/call answering group outbound calls.

The configuration steps are as follows:

Step 1 Click Go to Trunk > Analog trunk/IP trunk to select bundled trunk for extension/hunting group, and select DID for Inbound route.

 Copyright © Redstone Systems, Inc

Figure 2-38 Linear (DID) Configuration Screen



Step 2 Select drop-down list In the DID number field, enter and select the extension number or hunting group number that needs to be bundled.

Step 3 Select the Outbound call mode.

- Share: available for all extensions/call answering group numbers;
- DID only: The trunk can be used only by the specified extension or hunt group.

Step 4 Save the settings.

2.5.11 Binding Incoming Call Numbers to an Extension

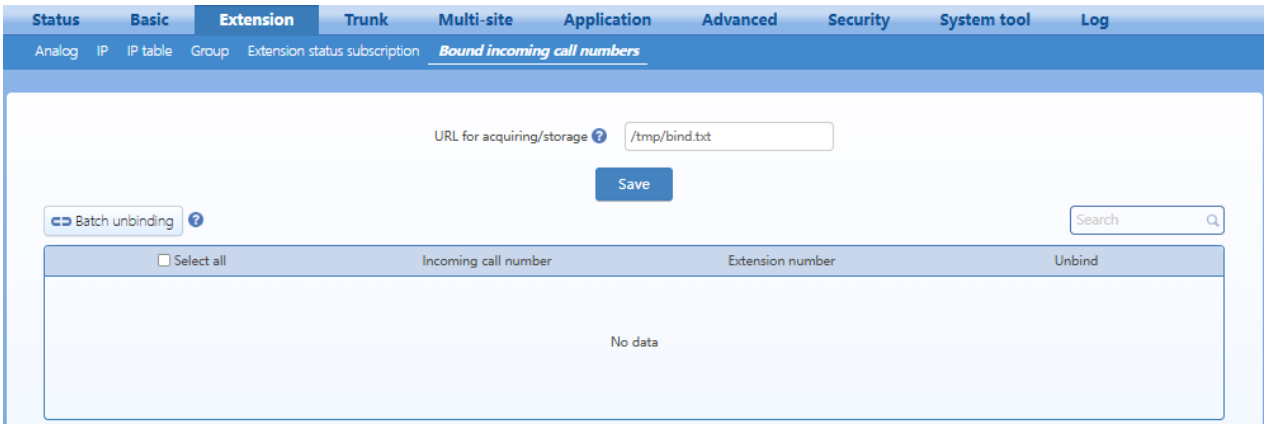
After binding an external caller's number to an extension, when that number subsequently dials the switchboard, the device will bypass the welcome message and go directly to the bound extension.

The extension can be tied to the caller's number by taking off the phone and dialing *66 after hanging up (you can dial *67 to unbind after tying up).

The binding relationship between an incoming call number and an extension can be viewed and canceled in the Extension Settings>Incoming Call Binding Numbers table on the device interface.

It is also possible to bind or unbind via the NeeHau Business Assistant (you need to enable NeeHau in the application services > API interface of your device).

Figure 2-39 Call Binding Number Table Interface



 Copyright © Redstone Systems, Inc

Table 2-24 Parameter Description of Caller Binding Number Form

Item	Definition
URL for acquiring/storage	The path where the device stores the binding relationship. The default path is /tmp/bind.ini, which can be modified.
Batch unbinding	Batch unbinding of numbers. Note: This button is not displayed when NeeHau is turned on in Application Services>API, and can only be unbound by NeeHau or the phone.
Search	Query number, support fuzzy query.
Incoming call number	Displays the phone number tied to the extension. Note: The interface is display only and cannot be configured.
Extension number	Displays the extension number to which the caller ID is bound. Note: The interface is display only and cannot be configured.
Unbind	Individual unbinding of numbers. Note: When Neehau is turned on, you can only unbind the relationship through NeeHau or the phone.

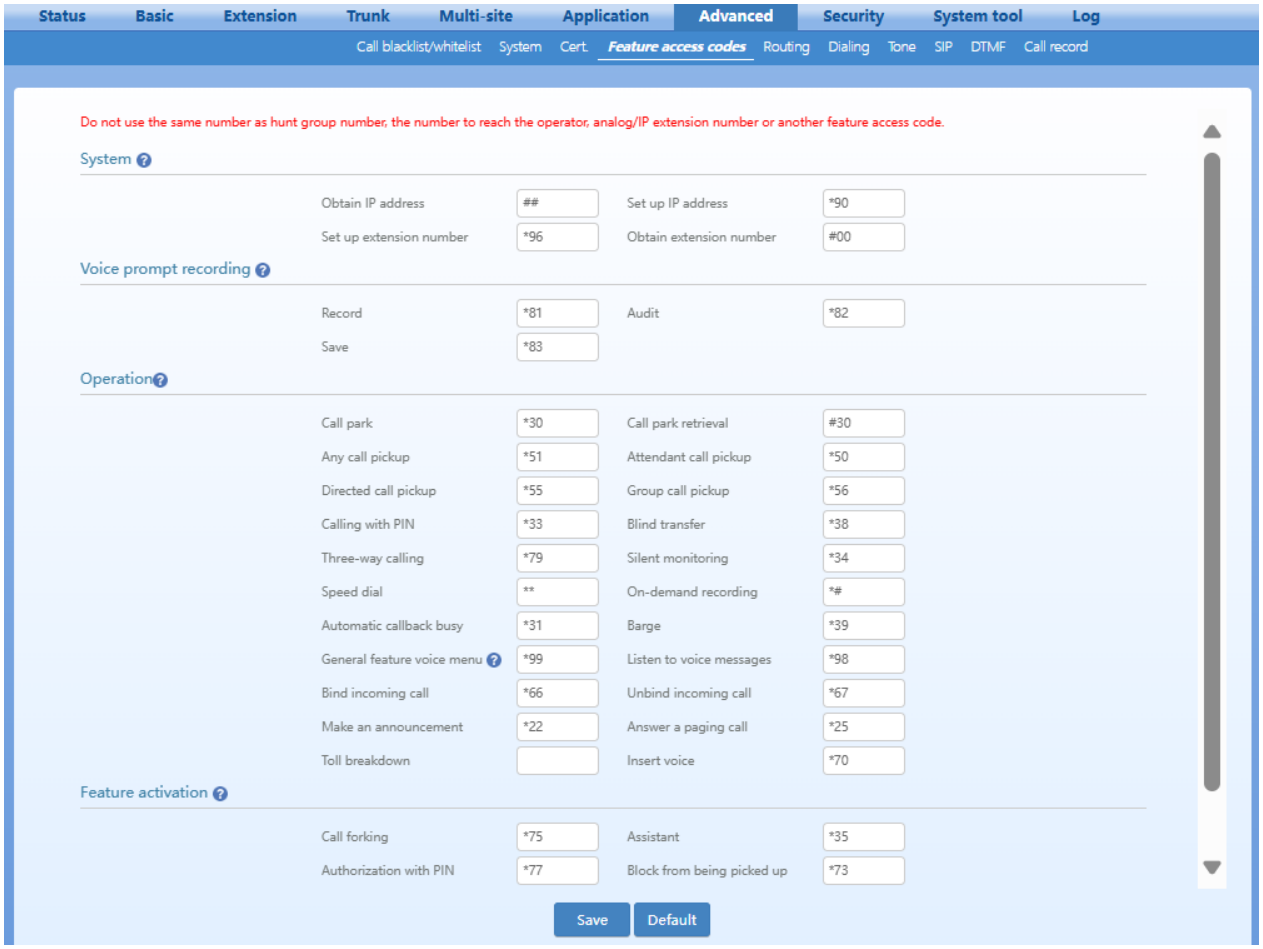
 Copyright © Redstone Systems, Inc

2.5.12 Function Codes

Click Advanced >Feature access Codes to query or customize the phone feature codes.

Click to view detailed help information for each function code.

Figure 2-40 Function Code Configuration Interface



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.

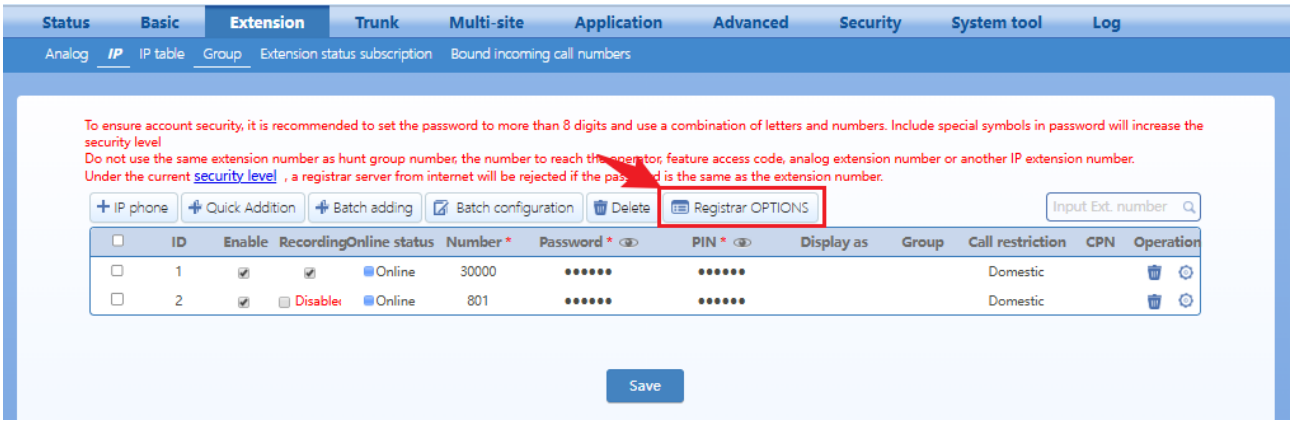
 Copyright © Redstone Systems, Inc

2.5.13 TLS Encryption

IP extensions support TLS encryption, users can enable TLS encryption and set TLS listening ports.

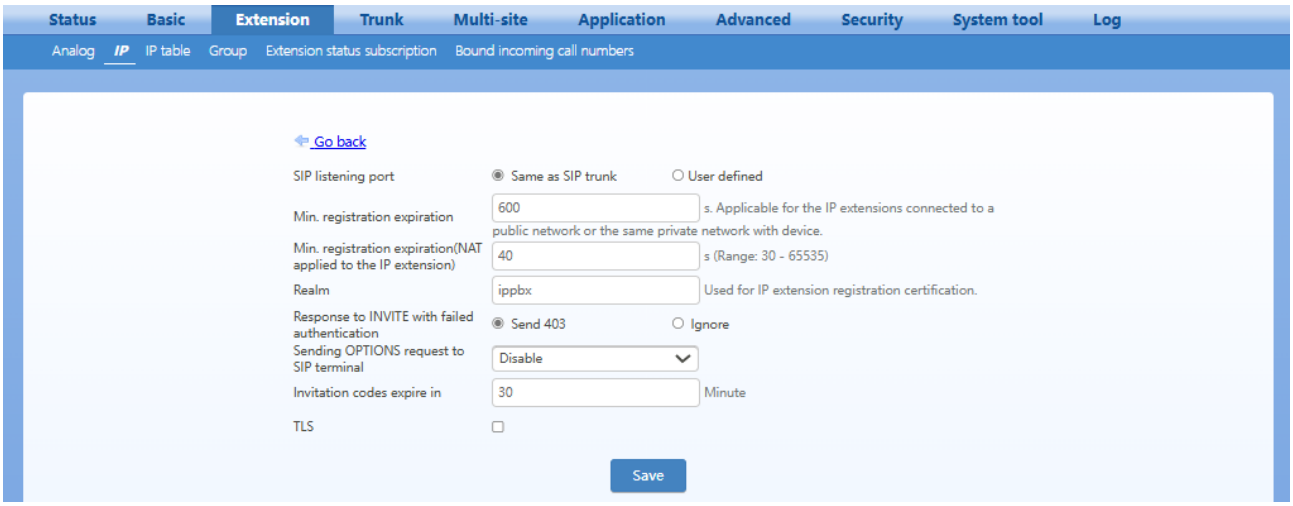
Step 1 On the Extension Settings > IP Extension page, click the "Registration Options" button.

Figure 2-41 IP Extension Setting Interface



Step 2 In the pop-up settings page, check the TLS option and set the TLS listening port.

Figure 2-42 TLS Settings Screen



2.6 Recordings and Messages

2.6.1 Recordings

REX supports G.711 and G.729 recordings. The REX20/REX50 has both remote recording and local recording, while the REX200/REX200-A/REX500/REX1000 only supports remote recording.

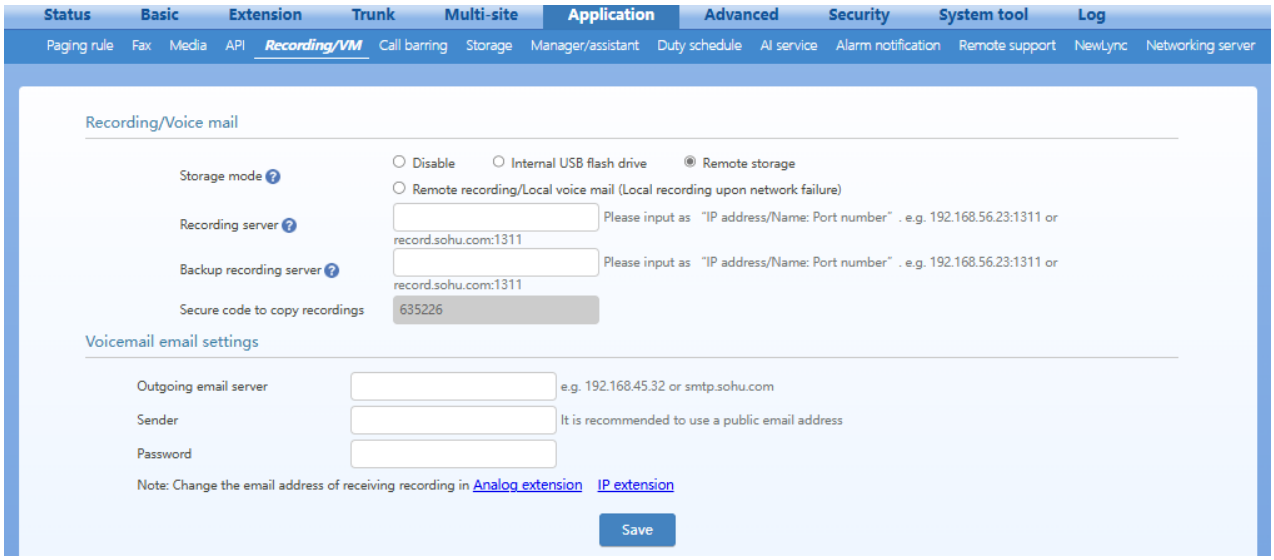
Remote Storage

The remote storage method is to store the recording files generated by the device in real time on a pre-deployed external recording server. The recording server is installed with the Redstone "Full Record" recording agent software or the Redstone recording management system.

The configuration steps are as follows:

Step 1 Click Application >Recordings/Messages and select Remote Storage.

Figure 2-43 Remote Storage Configuration Interface



Step 2 Fill in the IP address and port number of the recording server (default is 1311), e.g. 192.168.10.1:1311.

Step 3 Fill in the IP address and port number of the backup recording server (default is 1311), e.g. 192.168.10.1:1311.

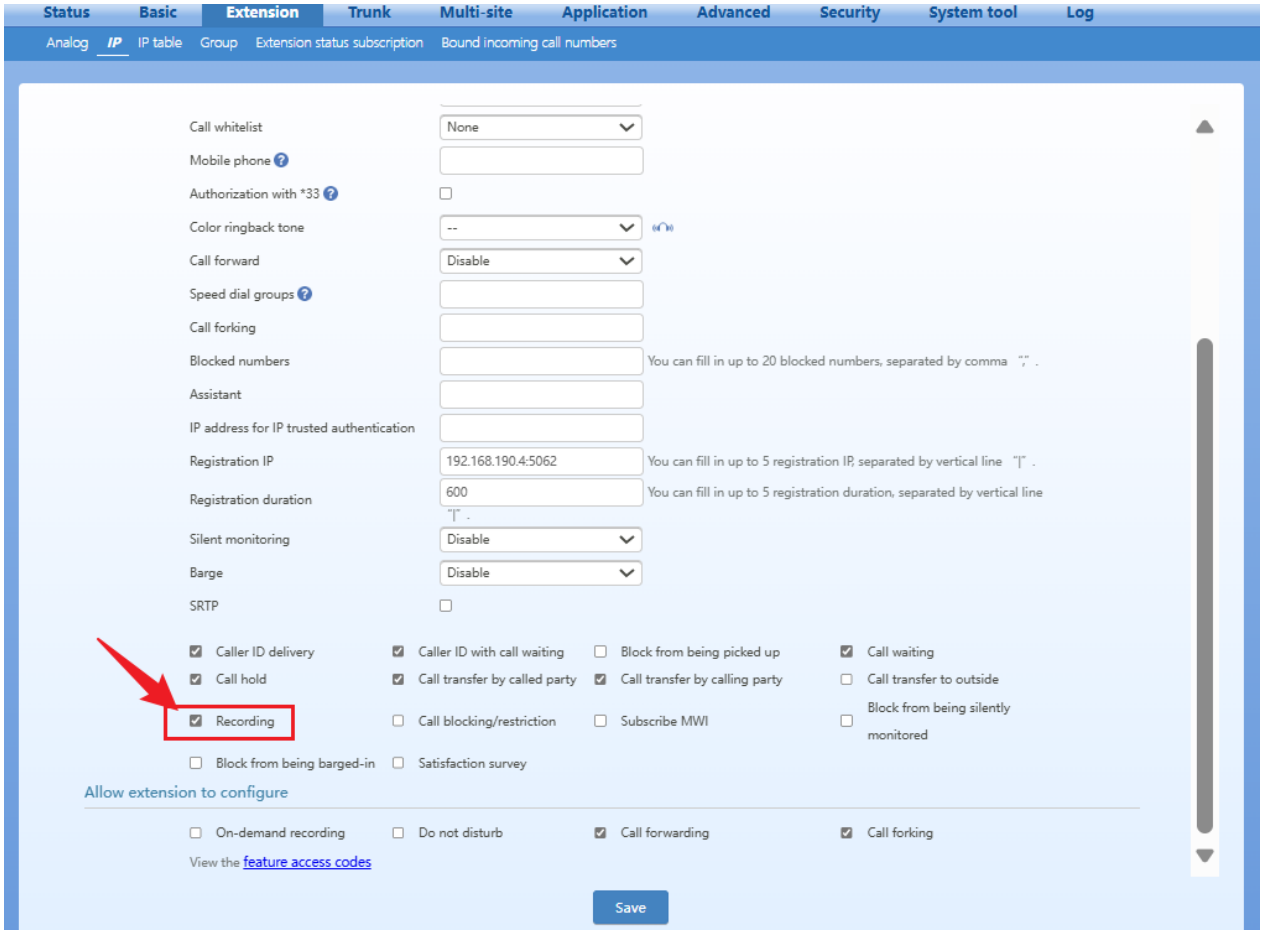
Step 4 Save the settings.

Step 5 Go to Extension >Analog Extension/IP Extension, select the extension that you need to enable the recording function, and click the Set button.

Step 6 Check the Recording in the Extension function.

 Copyright © Redstone Systems, Inc

Figure 2-44 Extension Recording Configuration Interface1



Step 7 Click Save.

Remote recording/local message (and local saving of disconnected recordings)

Remote Recording/Local Message is to save remote recording/local message (and local save disconnected recording) on remote recording server/backup recording server. The recording server is installed with the Redstone "Full Record" recording agent software or the Redstone recording management system.

The configuration steps are as follows:

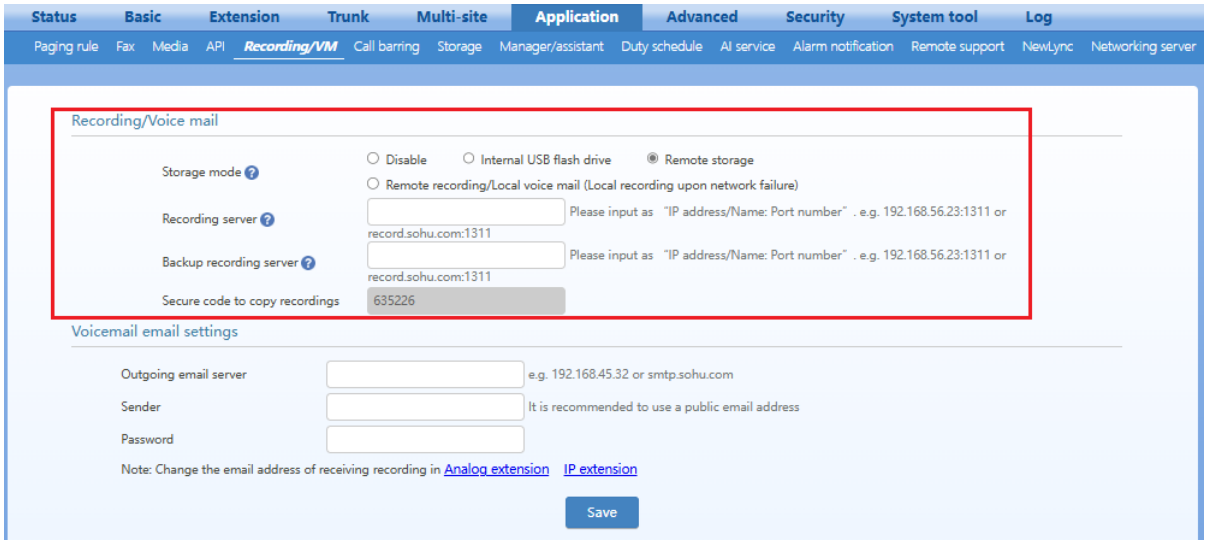
Step 1 Click Application >Recording/Messageand select Remote Recording/Local Message (and Local Save Disconnected Recording).

Step 2 Fill in the IP address and port number of the recording server (default is 1311), e.g. 192.168.10.1:1311.

Step 3 Fill in the IP address and port number of the backup recording server (default is 1311), such as: 192.168.10.1:1311.

 Copyright © Redstone Systems, Inc

Figure 2-45 Remote Recording/Local Message Configuration Interface

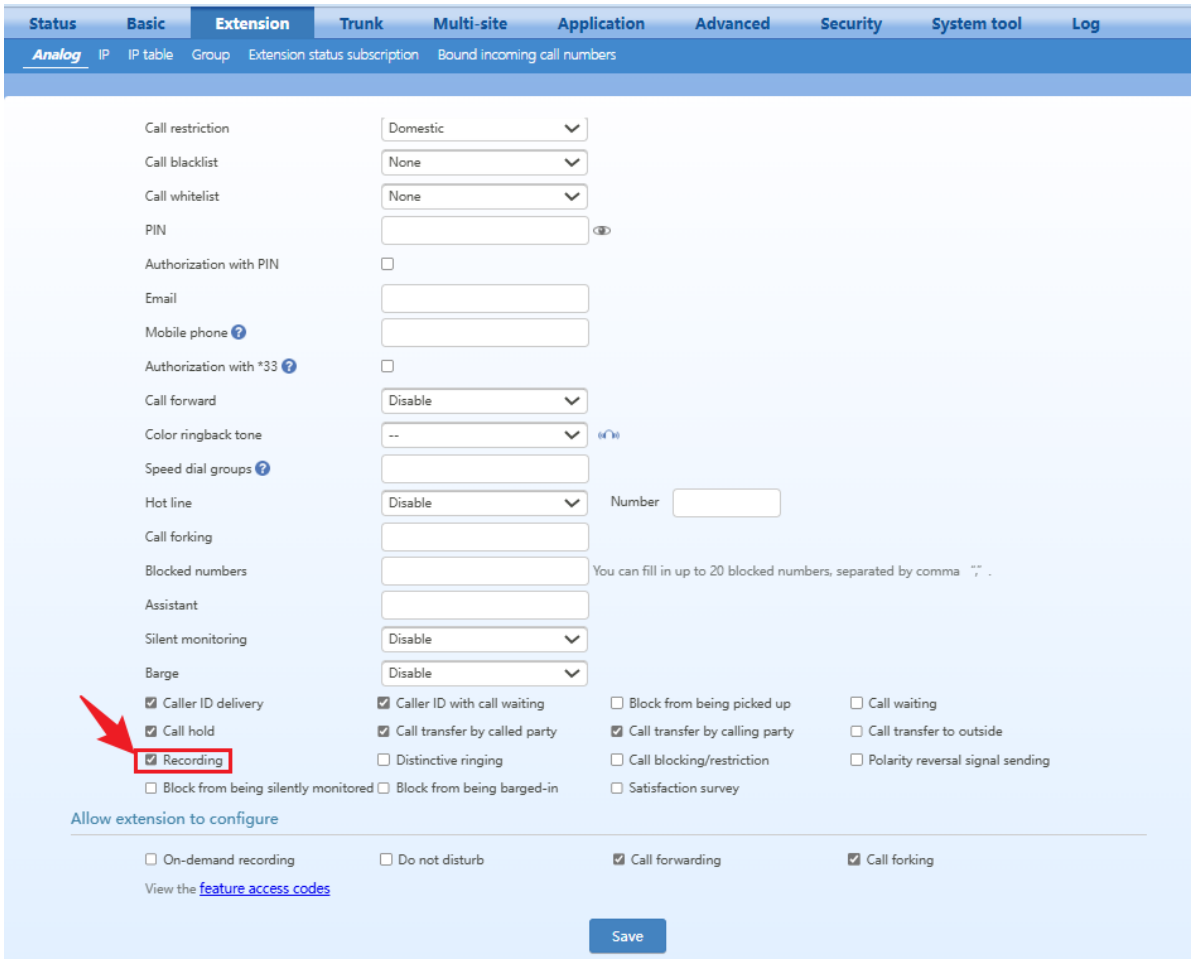


Step 4 Save the settings.

Step 5 Go to Extension >Analog Extension/IP Extension, select the extension that you need to enable the recording function, and click the Set button.

Step 6 Check Recording in the extension function.

Figure 2-46 Extension Recording Configuration Screen 2



 Copyright © Redstone Systems, Inc

Local recording (REX20/REX50)

Local recording is to save the recording file locally on the device, including the device's built-in storage or with a USB external storage device. The default storage space allocated for recording files in the built-in storage is 10240MB, the value can be found in Storage Management>Built-in Storage in Storage Management > Built-in Storage.

Note: Local recording files can also be backed up to a recording server, you need to enable backup to recording server.

Step 1 Enter the REX configuration interface and set the exact time in the System Tools > System Time interface. For specific settings, see 02.9.6 System time.

Note: Recording files are stored according to date and time, be sure to set the time correctly.

Step 2 In Application Services > Recording/Message, select Internal Storage or External USB Deviceas required. If an external USB deviceis selected, connect the USB storage device first.

Step 3 If the SIP server or IP Phones have Mute Suppression enabled, you must check Retain Original Recordings.

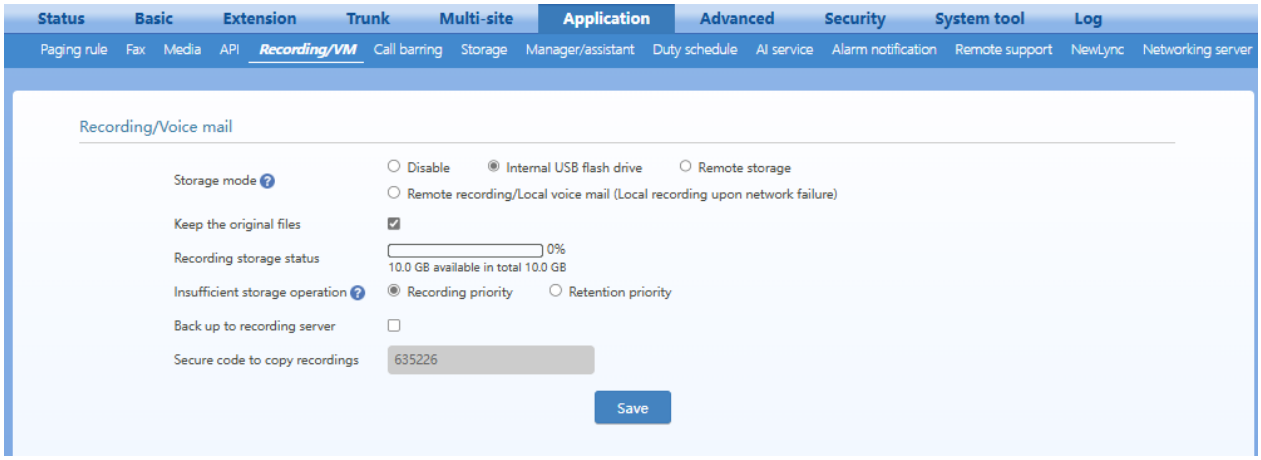
Step 4 Check Backup to Recording Server to back up local recording files to the recording server.

Step 5 Select the insufficient space treatment.

Cyclic Recording: Delete the recording files of the oldest day when the available storage capacity is lower than 500MB, or delete the earliest 100 recording files if there is only one day of recording.

Stop Recording: Stop recording when the storage capacity is full.

Figure 2-47 Built-in Storage Configuration Interface



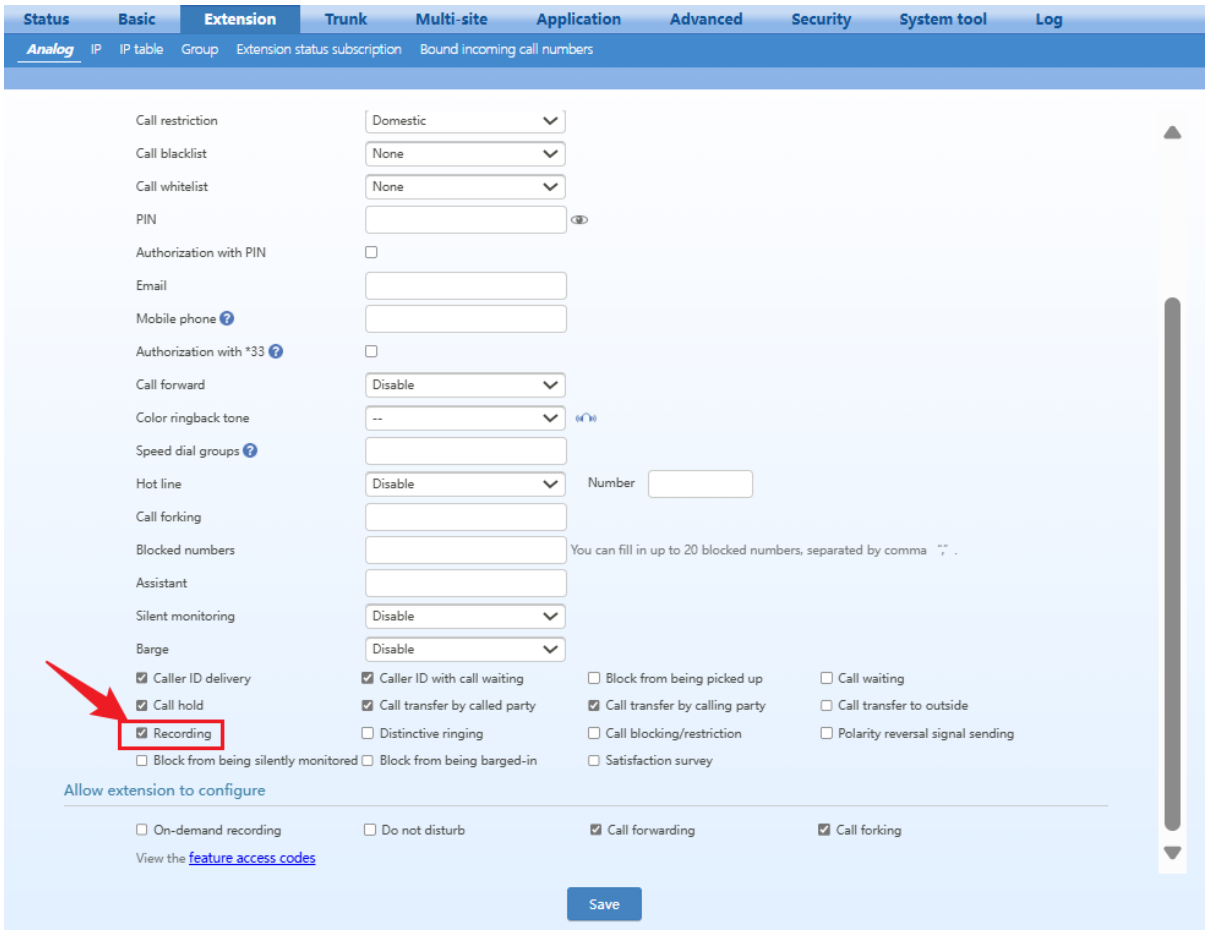
Step 6 Save the settings.

Step 7 Go to Extension >Analog /IP, select the extension that you need to enable the recording function, and click the Set button.

Step 8 Check the Recording in the Extension function.

 Copyright © Redstone Systems, Inc

Figure 2-48 Extension Recording Configuration Interface3



Step 9 Save the settings.

Managing audio files

Table 2-25 Managing audio files

File format	Caller_Called_Year_Month_Day_Hour_Minute_Second_Random_Code_cg.wav Caller_Called_Year_Month_Day_Hour_Minute_Second_Random_Code_cd.wav cg.wav is the recording file generated by the extension as the calling party cd.wav is the recording file generated by the extension as the called party For example: 200_80001_20121130_180028_a00a_cg.wav, represents the recording file generated on November 30, 2012 at 18:00:28 when extension 200 called number 80001.
View recorded files	• In Application Services>Storage Management, get the access path and then open that access path in a browser to view the recording files, built-in storage for builtin and external storage for usb. Recording files are stored in paths such as /Recorder/20140930, where 20140930 is a folder named after the month and year; • If the recording file is stored in external storage, you can also remove the storage device from the REX and connect it to the USB port of the computer to view the recording file. Recording files are stored in paths such as G:\Recorder\20140930, where 20140930 is a folder named after the month and year.

 Copyright © Redstone Systems, Inc

Listen to recorded files	Two ways to listen to audio files: • Follow the recording file view method to locate the recording file, download and listen to the recording; • Using the companion Business Assistant software, listen to the recording on the Business Assistant Call Log screen.
Backup and clear recorded files	• Built-in storage: Click Backup under Application Services > Storage Management to backup all the recording folders Recorder in the built-in storage to the root directory of the external USB device. Click Clean upafter backup to delete the recording files from the built-in storage. • External Storage: Remove the USB storage device and connect it to a computer for backup and cleanup.

2.6.2 Messages

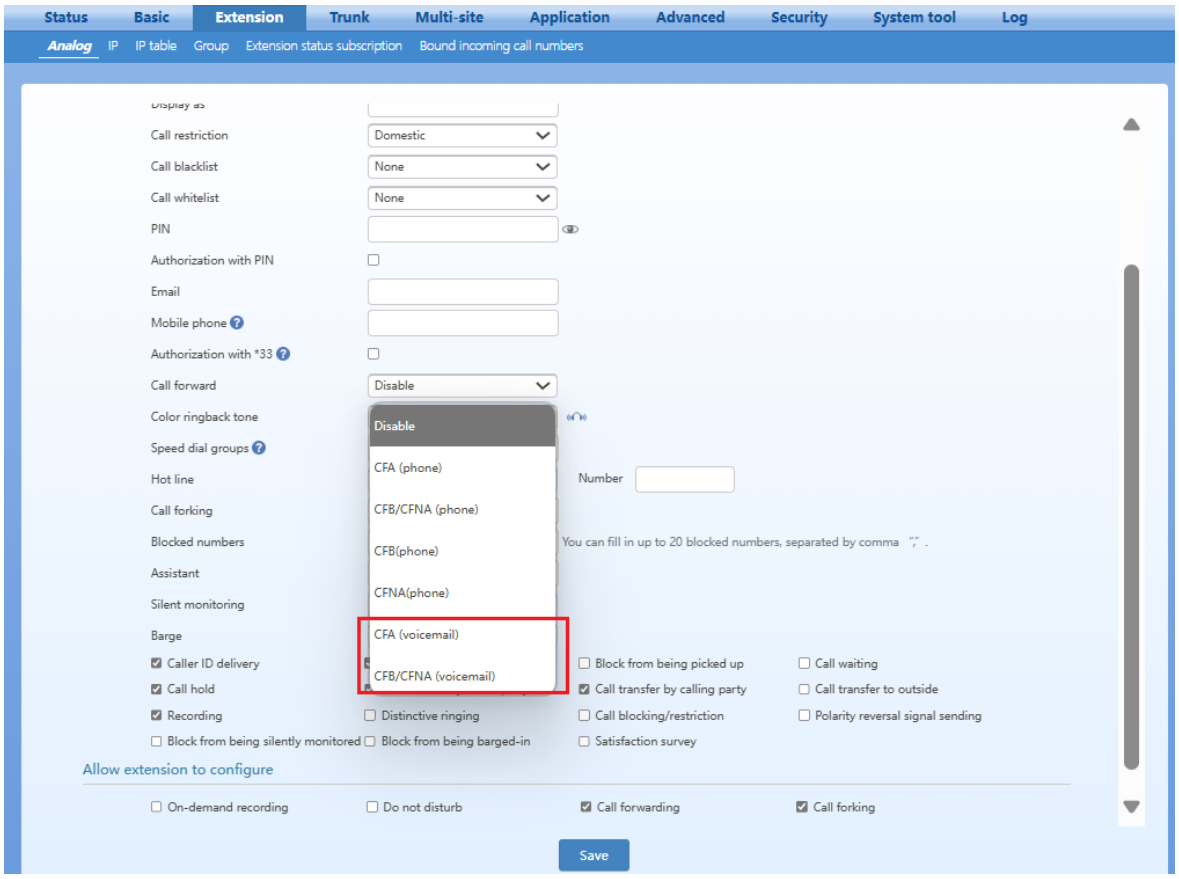
After turning on the message function, when the extension user cannot answer the incoming call, the other party can leave a voice message after the voice prompt.

Step 1 Tap Application Services>Recording to enable the recording function. For details, please refer to 02.6.1 Recordings. The location where the message file is stored is related to the recording, i.e. If the recording method is selected as internal storage, the message file will also be stored in the internal storage.

Step 2 Click Extension >Analog /IP >Setup to select Call Forwarding Method as All Incoming Calls to Voice Message or Busy/No Answer to Voice Message.

 Copyright © Redstone Systems, Inc

Figure 2-49 Message Configuration Interface



Step 3 Save the settings.

When the recording method is remote storage, the message file can be sent to the extension user's mailbox. Configure it as follows:

Step 1 Select the recording method as Remote Storage, configure the Recording Server/Backup Recording Server address and port number, and configure the voice message email sending server.

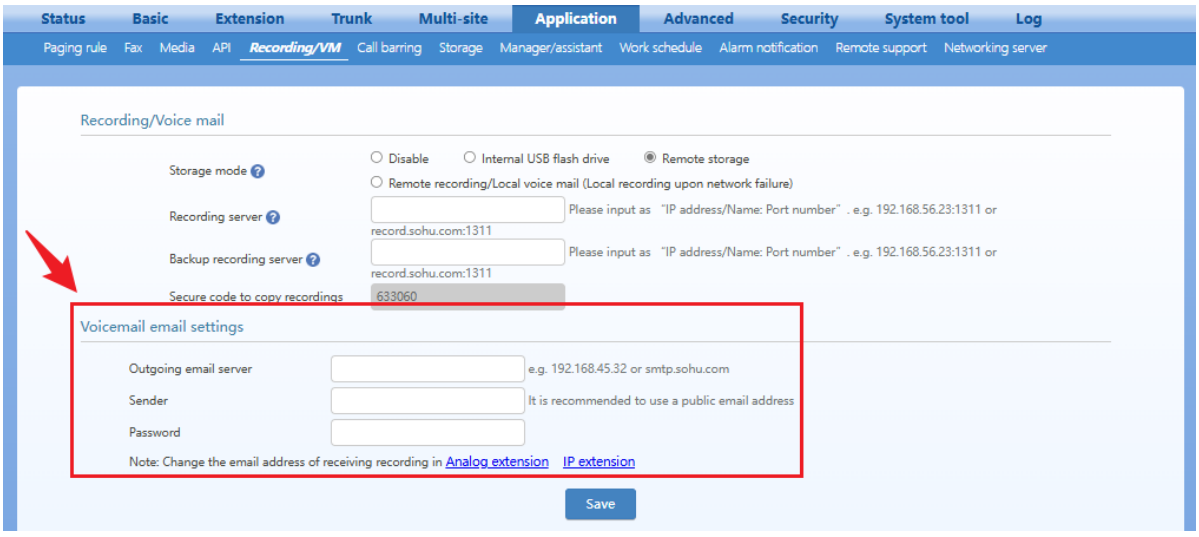


Table 2-26 Parameter description of voice message sending server

Item	Definition
Outgoing email server	Fill in the address of the mail delivery server. The device supports Sina and Sohu mailboxes.
Sender's email	Fill in the sender's e-mail address.
Password	Fill in the sender email password.

Step 2 Save the settings.

Step 3 Go to Extension >Analog Extension/IP Extension>Settings to configure the mailbox that will be used as the inbox for receiving voice message files.

Step 4 Save the settings.

Manage Message Files

Table 2-27 Manage Message Files

File format	The name of the voice file for the new message is: vm_called-caller-random-code.pcm, e.g.: vm_200-6033432345-946685192.pcmm. If you press Listen Again, Next, or Listen to End Message while listening to a new message, the device recognizes this voice file as listened to and the file name changes tooldvm_200-6033432345-946685192.pcm. Note: When the speech codec is G.711μ, the suffix is. pcm; when the speech codec is G.711 a, the suffix is. pcma; when the codec is G.729, the suffix is .dat; when the codec is G.722, the suffix is. g722; and when the codec is G.722.2, the suffix is. g722B.
View the voicemail message files	• In Application Services > Storage Management, get the access path, then open that access path in a browser to view the message file, built-in storage built in, external storage usb. Message file storage path such as /Recorder/voicemail; • If the message file is stored in external storage, you can also remove the storage device from the REX and view the file after connecting it to the computer's USB port. The path where the message file is stored is such as G:\Recorder\ voicemail.
Listen to the voicemail message files	• Analog Phones: Use the phone function code to listen to messages on an extension. Take off the phone + *98 to enter the mode of listening to the message, there will be voice prompts during the listening process: "You have no voice messages" or "You have n new/old voice messages, press # to listen to messages; to listen to messages, press 1 to re-listen, 2 to delete, 3 to next". After listening to each message, there will be a voice prompt: press 1 to listen again, press 2 to delete, and press 3 for the next message. • IP Phones: To listen to a message on an IP phone, you need to set the memory key and MWI function key first, and then listen to the message using the function code. Refer to the NRP Phones User's Manual for specific settings.
Backup & cleanup messages	Same Managing Recording Files.

2.7 Fax

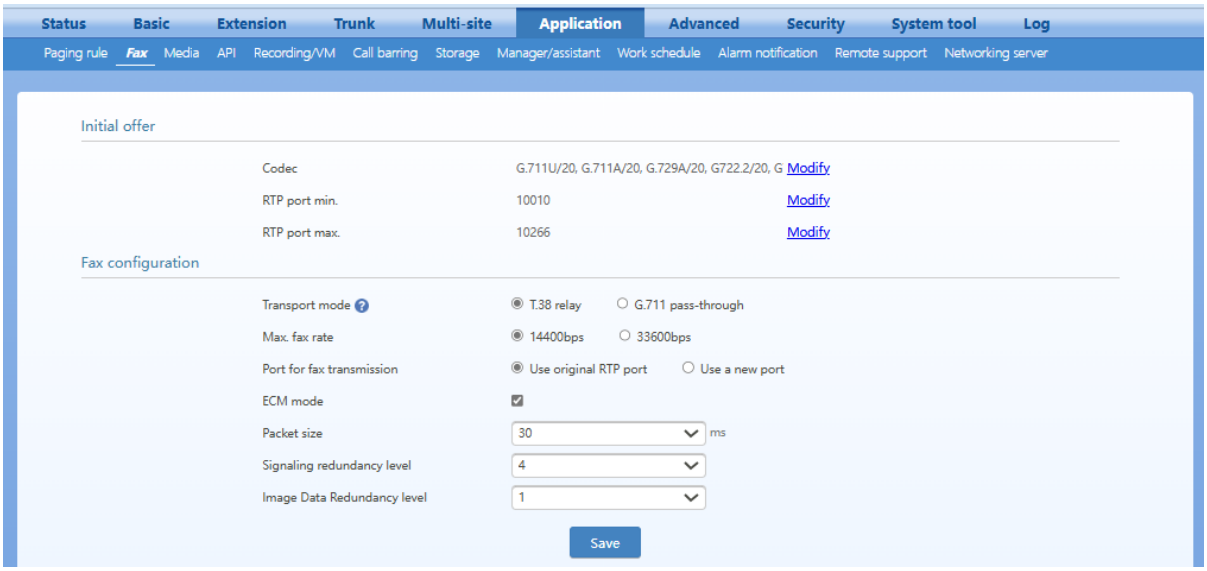
The fax machine can be used by connecting a telephone line directly to the FXS port of the REX, or it can be used by connecting to the FXS port of a gateway registered to the REX. When sending a fax, just dial the fax number by calling an outside line.

Click Application >Fax to configure faxing.

Figure 2-50 Fax Mode Configuration Interface (REX20/REX50)



Figure 2-51 Fax Mode Configuration Interface (REX200/REX200-A/REX500/REX1000)



 Copyright © Redstone Systems, Inc

Table 2-28 Fax Interface Parameter Description

Item	Definition
Initial offer	Set the maximum and minimum values of codec and RTP port, click "Edit" to jump to the media page for configuration. For more information, please refer to Table 2-42 Description of media parameters. Note: When using G.711 Transmissive, you need to select G.711U/20 or G.711A/20 correctly in the codec.
Transport mode	The device supports two fax modes: T.38 and G.711 pass through. When fax is received or sent through analog outside line, G.711 transmission mode should be used; when fax is received or sent through IP outside line, T.38 or G.711 transmission mode can be selected according to the mode supported by IP telephony operation platform and the actual need, if the platform supports both modes, T.38 mode, which is more stable in transmission, is recommended to be used.
Max. fax rate	Select the maximum transmission rate that can be achieved when faxing, 33600bps for high-speed fax mode.
Port for fax transmission	Whether to enable the new RTP port when the device switches to T.38 mode, the default is to follow the original voice port, it is recommended to use the default configuration. • Enable New Port: Use the new RTP port; • Follow the original voice port: Use the original RTP port that was used when the call was established.
ECM mode	Use the fax error correction mode. The default value is related to the transmission rate: ● REX20/REX50: The default is not on when 14400bps is selected for the maximum transmission rate, and the default is on when 33600bps is selected; ● REX200/REX200-A/REX500 /REX1000: Not enabled by default.
Output gain control (REX200/REX200-a/REX500/REX1000)	Sets the amount of increase or decrease in T.38 fax transmission gain. The range of values is -6 to +6 dB, and the default value is 0 dB. -6 dB indicates 6 dB attenuation; +6 dB indicates 6 dB amplification.
Packet size	Sets the T.38 data frame packet interval, selectable from 30 ms or 40 ms, the default value is 30 ms.
Signaling redundancy level	Set the number of data redundancy frames in T.38 packets, the value range is 0~6 frames, the default value is 4 frames.
Image Data Redundancy level	Set the number of data redundant frames in T.38 packets, the value range is 0~2 frames, the default value is 1 frame.
Allow opposite terminal to switch to T.38	After checking, when this device acts as a fax sender and the fax mode is G.711 passthrough, if the other end initiates a T.38 negotiation request, this device will respond to the request and switch to T.38 mode automatically.
Receiving terminal (REX200/REX200-A/REX500/REX1000)	• Send Re-INVITE. Codecs are automatically selected based on the Re-INVITE negotiation results. • Transmission: To ensure proper fax functionality, make sure G.711U/20 or G.711A/20 is selected in the codecs

 Copyright © Redstone Systems, Inc



It is recommended to configure a DID line for fax extensions, for more information, please refer to 02.5.10 .

2.8 Multi-Device Networking

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.

There are two options for assigning extension numbers to devices within the network: 1) unique extension numbers for the entire network; and 2) independent setting of extension numbers for each device. The networking configuration and dialing methods of these two number planning schemes differ and are described below.

2.8.1 Assign the extension numbers globally

With this program, since the extension number is unique in the whole network, extensions dial each other directly without prefixing each other's extension number.

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

This approach is suitable for stacking multiple devices to achieve capacity expansion, or deploying multiple devices in different geographical areas to achieve small-scale networking. It is not suitable for large-scale networking between headquarters and branches under a hierarchical management model.

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

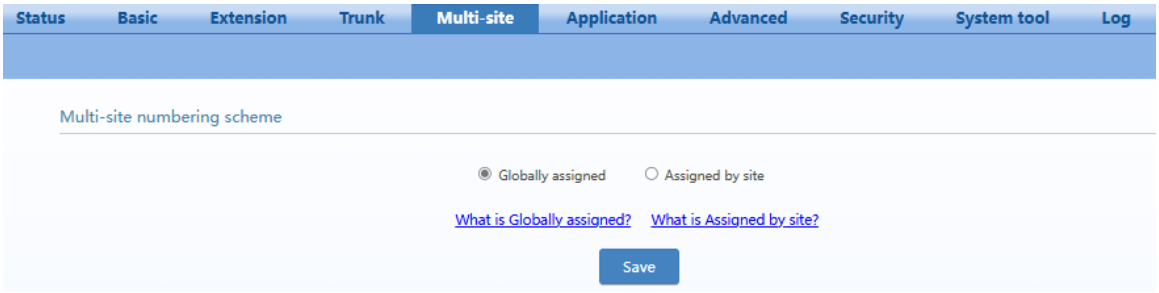
site. Each common site only needs to configure the management site and its own information, so that it can periodically get information about other sites from the management site.

See below for detailed configuration Definition.

Managing the site

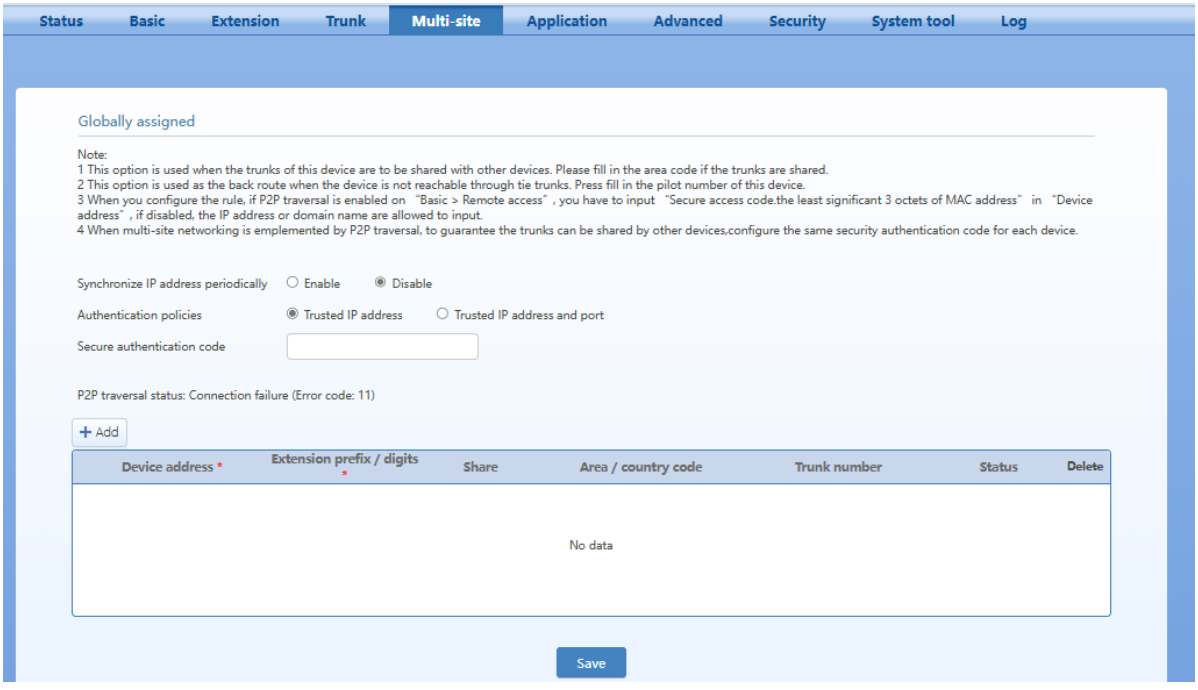
Step 1 Go to Network Settings, select Number Unique, and click Save to enter the configuration page.

Figure 2-52 Networking Solution Selection Interface



Step 2 Enable periodic synchronization of device addresses on the network.

Figure 2-53 Network Configuration Interface



Step 3 Select the security policy. the REX provides two authentication methods.

Table 2-29 Security Policy Parameters

Item	Definition
Trusted IP address	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.
Trusted IP address and port	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.

Step 4 Adding a management site

Click New and enter the management site information.

Figure 2-54 Add Site Interface



Table 2-30 Site Add Interface Parameters

Item	Definition
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 entry is for the management site, and the management site IP address must be fixed. Others are common site, if the IP address of the common site is dynamic, fill in the domain name of the common site device here, and the value is the same as that of the common site device. Remote accessconfiguration. The device address can be configured as asecurity access code if penetration is enabled under Basic Settings > Extranet Access. The last six digits of the MAC, for example 996725.3D1727, indicate that networking is done by penetration. Note: If the device is in the private network and does not open the penetration function, you need to do port mapping on the front-end router, please refer to the Remote access Please refer to the "Port Mapping Methods" in the following section. Port Mapping Please refer to the port mapping method below.
Extension prefix/number digits	Enter a range of extension numbers for the device, e.g., 2/3 means that 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, if Device A and Device B have prefixes 2/3 and 21/3, respectively, and if both devices have extension 210, users of Device A cannot dial to Device B's extension 210, and calls dialing 210 are sent to Device A's extension 210.
Share	• 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 /Country 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 repeated). For example, site A fills in the area code 8, allowing its outside line to be shared with other sites in the network, and other sites can call 861202777 when calling number 61202777, which is played through site A's outside line, and site A will automatically remove 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).
Trunk number	When an extension of another device in the network calls the extension of this device during a network outage, it can call this device through PSTN by calling "area code + the number".

Step 5 Add another site

Click Add to add information about all general site equipment on the net. For a description of the parameters see Table 2-30.

Step 6 Update device address

Step 7 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

 Copyright © Redstone Systems, Inc

the other devices.



- If the IP address of the general site is dynamic, the management site needs to be configured with a fixed IP and the device address of the general site needs to be configured with a domain name.
- Incorrect DNS can lead to wrong IP address acquisition, it is recommended to disable the DNS service.

General site

Step 1 Go to Network Settings, select Number Unique, and click Save to enter the configuration page.

Step 2 Enable periodic synchronization of device addresses on the network.

Step 3 Select the security policy.

Step 4 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.

Step 5 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.

Step 6 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.

2.8.2 Repeatable extension numbers within the network

Avoiding number conflicts by dialing specific prefixes when extensions are dialed to each other makes it possible to duplicate extension numbers under different sites. This kind of network can satisfy the demand for hierarchical self-management of equipment numbers of headquarters and branches, and thus is suitable for the voice network of large and medium-sized group organizations.

 Copyright © Redstone Systems, Inc

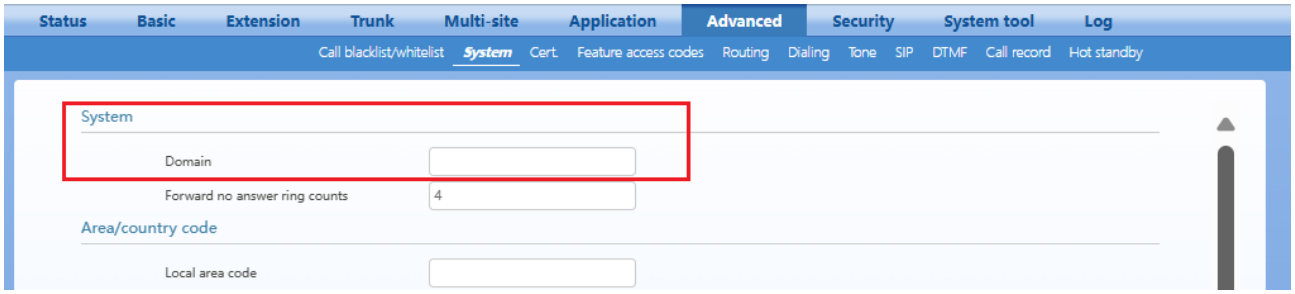
Managing the site

Select one of the devices in the network as the management site, which uniformly allocates dialing prefixes and outgoing resources in addition to sending address change information of any device in the network to other devices in a timely manner. The following describes the procedure for setting up the network for the management site.

Step 1 Enter the local domain name.

Click Advanced >System, enter the IP address or domain name of this device at Local Domain Name and click Save.

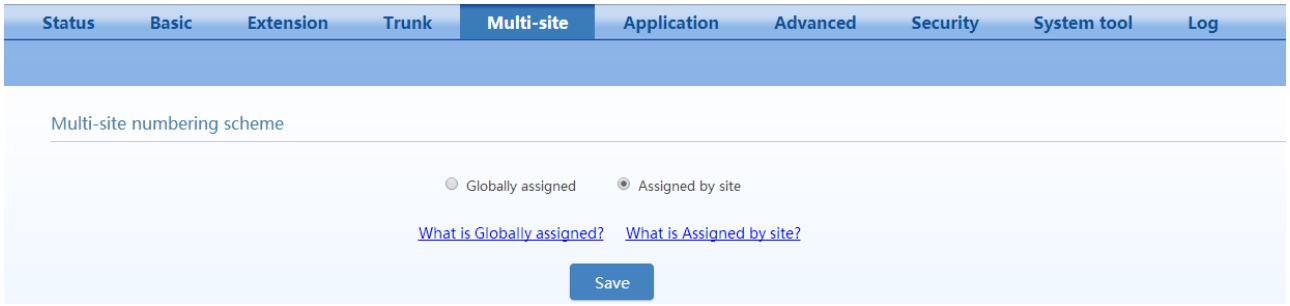
Figure 2-55 Management Site Local Domain Name Configuration Interface



Step 2 Select the networking mode.

Click Network Configuration, select Number Repeatable, and click Save.

Figure 2-56 Management Site Network Configuration Interface 1



Step 3 Select the role of the device in the grouping

Select Manage Sites and click Save.

 Copyright © Redstone Systems, Inc

Figure 2-57 Select Device Networking Role Interface

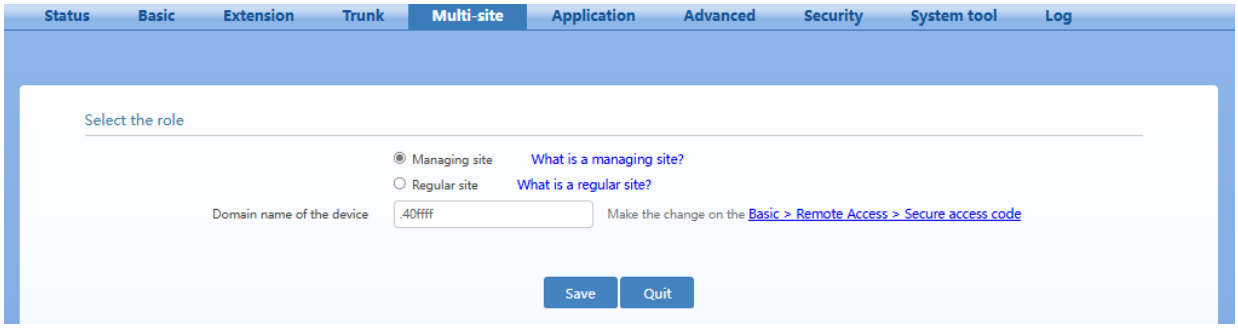
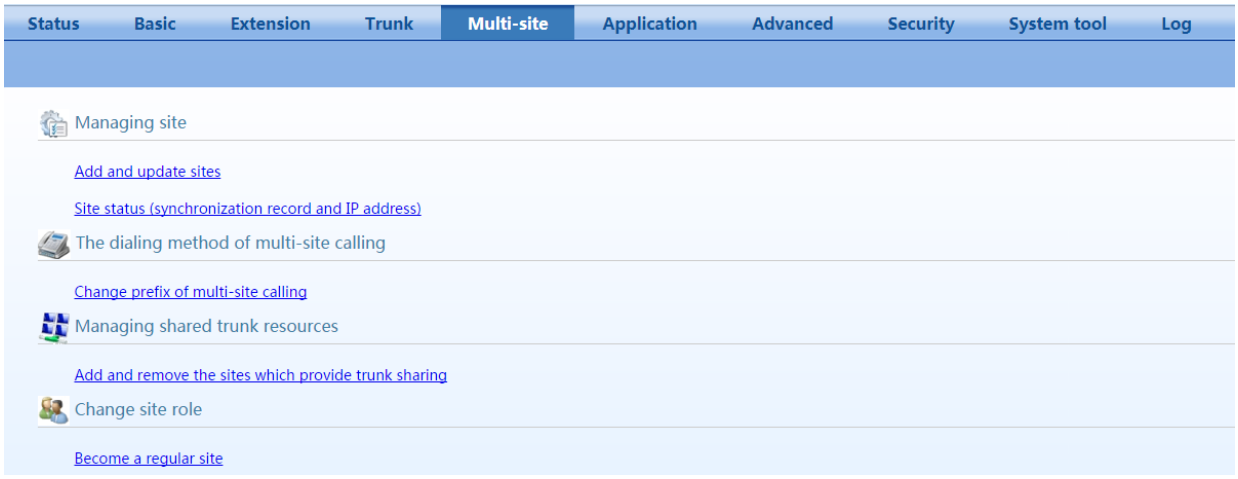


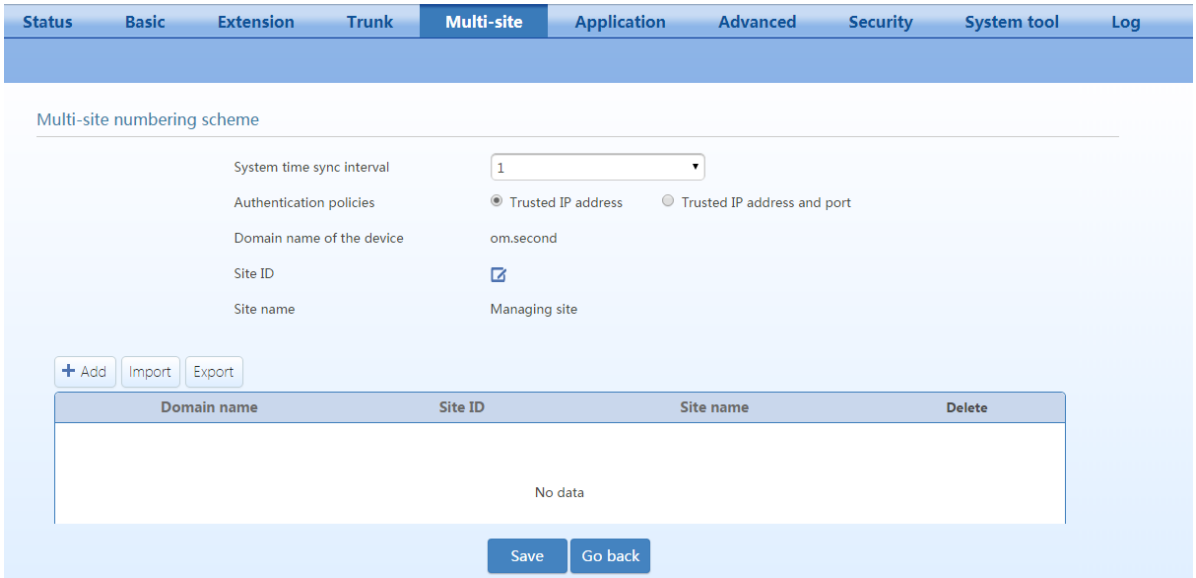
Figure 2-58 Management Site Configuration Interface 2



Step 4 Adding and modifying site information

After clicking the Add and Modify Site Information link under the Manage Group Sites point, click Add.

Figure 2-59 Management Site Network Configuration Interface 3



 Copyright © Redstone Systems, Inc

Table 2-31 Description of the parameters of the network planning interface

Item	Definition
System time sync interval	Cycles synchronized with normal sites.
Authentication policies	• Site IP authentication: only the device IP address needs to be authenticated. • Site IP+Port Authentication: The device IP address and SIP port number need to be authenticated. For more information, see Table 2-29 Security Policy Parameters.
Domain name of the device	The IP address or domain name of this device. This can be modified in Advanced Settings > System > Local Domain.
Site ID	Fill in the site number of the management site, which is used to identify each other when calling between grouped devices. The numbering can be arbitrary, but not duplicated.
Site name	The role of this device in the grouping.
Add	
Domain name	Add the common site identity (consistent with the local domain name configured on the common site), i.e. common site IP + port number. If you do not fill in the port number, the default port 5060 will be used. When the security policy is "Site Identity + Port Authentication", you must ensure that the port value is filled in correctly. Go to Outbound Settings > SIP Outbound > Registration Options, and you can modify the SIP port inLocal Port.
Site ID	Fill in the site number of a common site for mutual identification when calling between networked devices. The numbering can be arbitrary, but not duplicated.
Site name	The site's role in the grouping. Such as common sites.
Delete	Delete the current site information.

Step 5 Modify the group dialing prefix

Return to the Management Site Configuration screen and set the networking dialing prefix after clicking the Modify networking dialing prefix under Networking dialing method link.

 Copyright © Redstone Systems, Inc

Figure 2-60 Management Site Network Configuration Interface 4

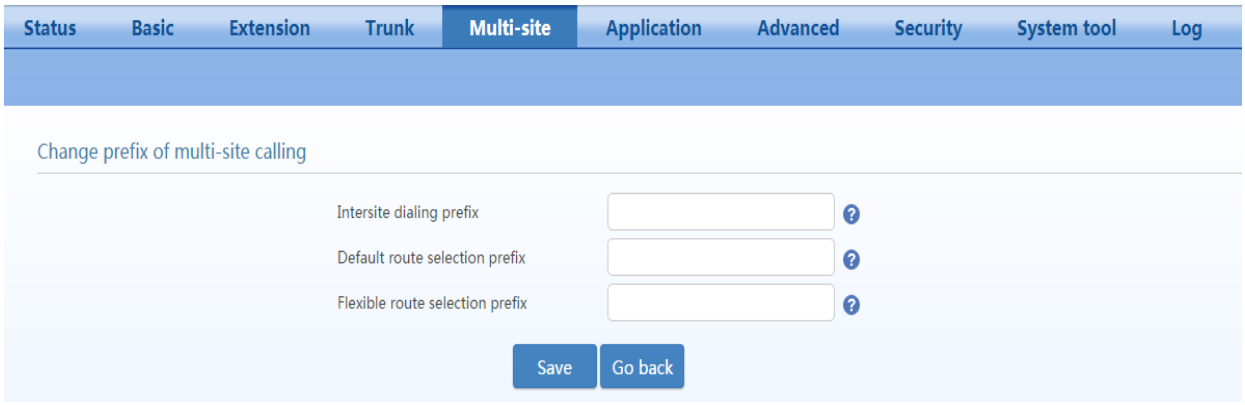


Table 2-32 Networking Dialing Prefix Interface Parameter Description

Item	Definition
Inter-site dialing prefix	Used to dial an internal line, e.g., # + inter-site extension inter-dial prefix + site number + opposite end extension number.
Default route selection prefix	Used to dial an outside line, e.g., # + auto-select outgoing site prefix + outside number.
Flexible route selection prefix	Used to dial an outside line, e.g., # + specified outgoing site prefix + site number + outside line number.

Step 6 Configure the external line sharing method

Return to the Management Site Configuration screen and configure the relevant information in the Outbound Resources screen after clicking on any of the links under Management Shared Outbound.

Figure 2-61 Management Site Network Configuration Interface 5

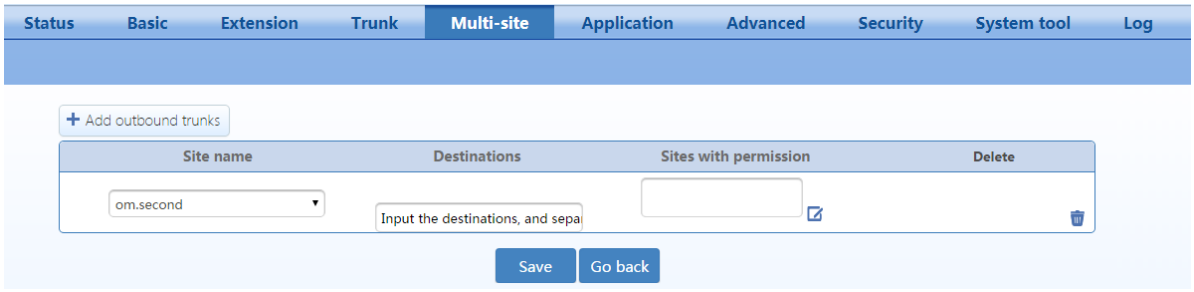


Table 2-33 Description of Outgoing Resource Interface Parameters

Item	Definition
Site name	Sites that provide outbound line sharing give outbound lines to devices that are allowed to share that outbound line according to the default first rule on the Device Outbound Rules screen.
Destinations	The area code of the area where dialing is allowed, with multiple area codes separated by ",".
Sites with permission	Select the stations that can use this outbound resource outbound.

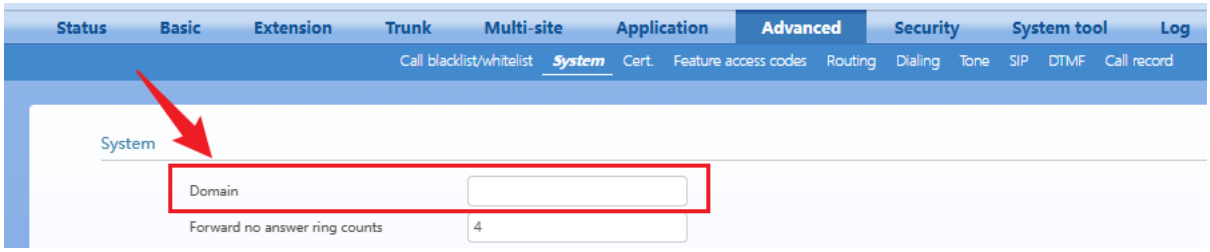
 Copyright © Redstone Systems, Inc

General site

The configuration steps for the other sites in the network are simpler than those for the management site.

Step 1 Click Advanced > System, enter thelocal domain name of the common site and click Save.

Figure 2-62 Common Site Local Domain Configuration Interface



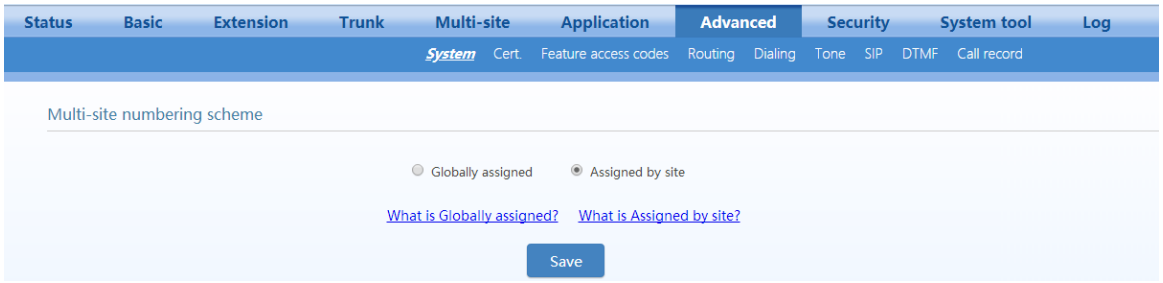
Note

- If the local domain name has already been set, you can skip to "Step 2".
- When networking, you need to report the local domain name and port of the common site to the management site.

Step 2 Selecting the Networking Mode

Click on Network Settings, select Number Repeatable and then click Save.

Figure 2-63 Common Site Networking Configuration Interface 1

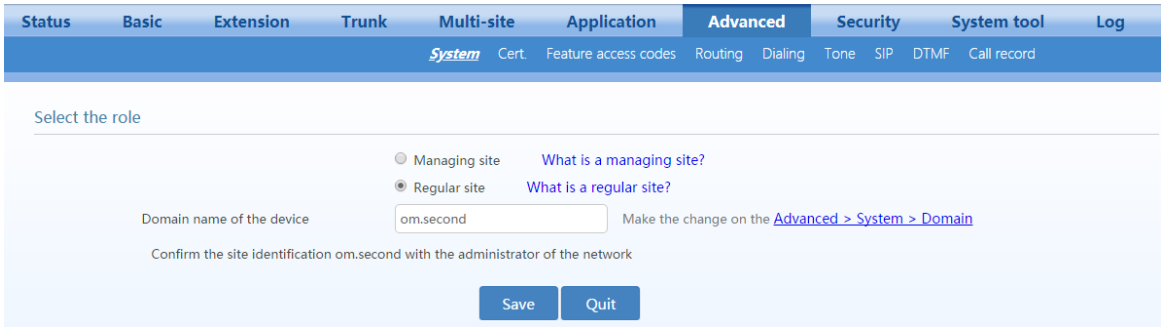


Step 3 Select the role of the device in the grouping

After selecting General Site, click Save.

 Copyright © Redstone Systems, Inc

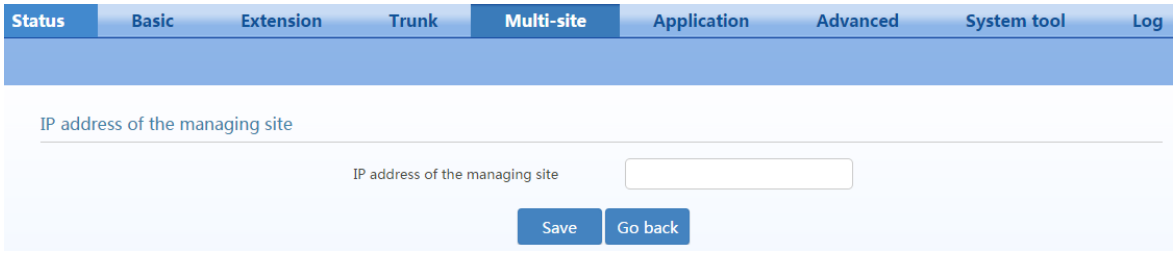
Figure 2-64 Common Site Networking Configuration Interface 2



Step 4 Enter the management site IP address

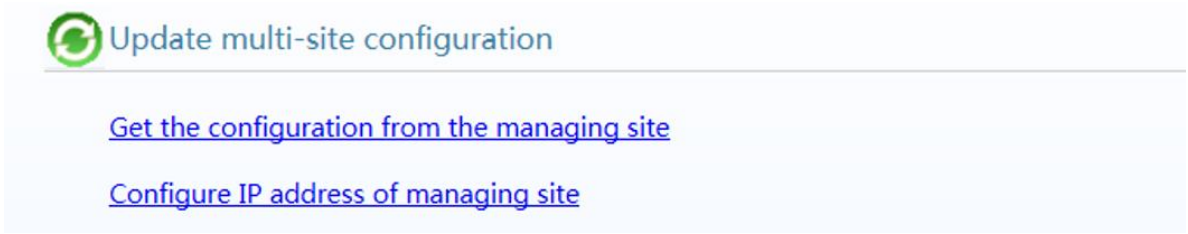
After clicking the Configure Management Site IP Addresses link under Automatically Obtain Networking Information, enter the management site IP address.

Figure 2-65 Common Site Networking Configuration Interface 3



Displays green after a successful connection to the management site.

Figure 2-66 Common Site Networking Configuration Interface 4



2.9 System Configuration

2.9.1 Built-in storage management

The REX20/REX50/REX200/REX200-A/REX500 have 16GB of built-in storage, and the REX1000 ship with a 32GB memory card (starting in 2018).

The REX20/REX50's built-in storage is used for storing recordings, messages, logs, voice files, and more.

The built-in memory of the REX200/REX200-A/REX500/REX1000 is used to store logs. The data in the built-in storage is not lost after the device is rebooted.

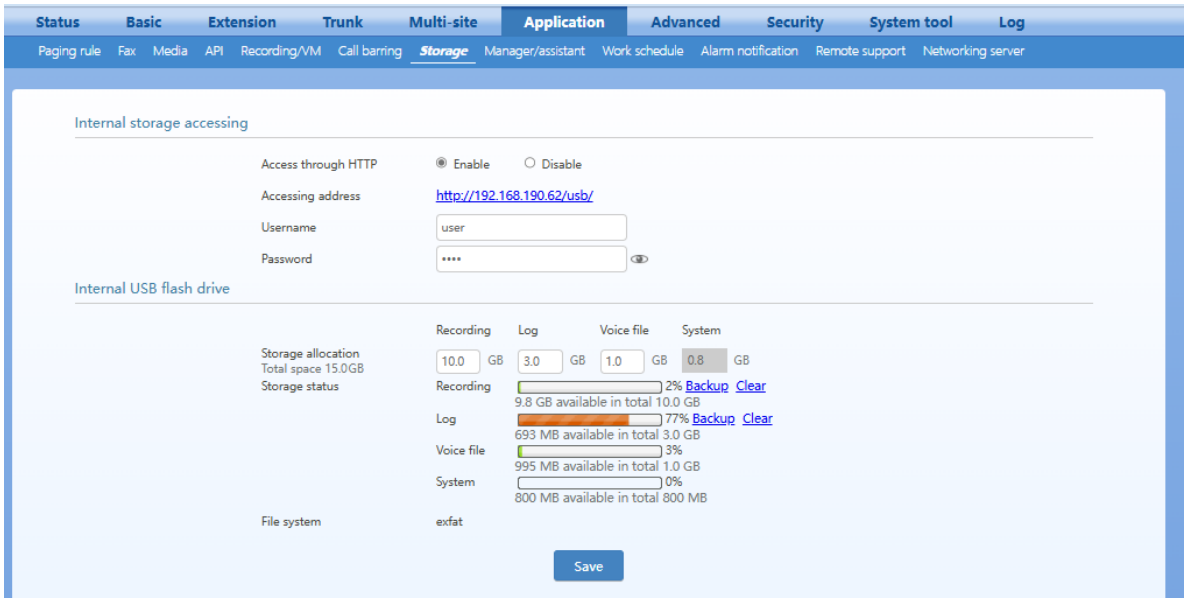
Go to Application > Storage Management to manage the built-in storage space of REX20/REX50. The default space allocation is as follows:

Item	Space
sound recordings	10 GB
log (computing)	3 GB
voice file	1 GB
other than	0.8 GB

If the REX20/REX50 requires expansion of the storage space, an external storage device can be connected through the USB port of the device. By clicking Backup, you can back up your recording files to an external storage device and clean up the internal storage. Before backing up, make sure there is enough space on the external storage device.

 Copyright © Redstone Systems, Inc

Figure 2-67 Built-in Storage Management Interface



2.9.2 Incoming call duty roster

Incoming Call Duty List helps you to answer incoming outgoing calls from different duty cell phone numbers at different times of the day.

Step 1 Application > Duty Schedule, click Add New Duty List.

Figure 2-68 Duty List Screen

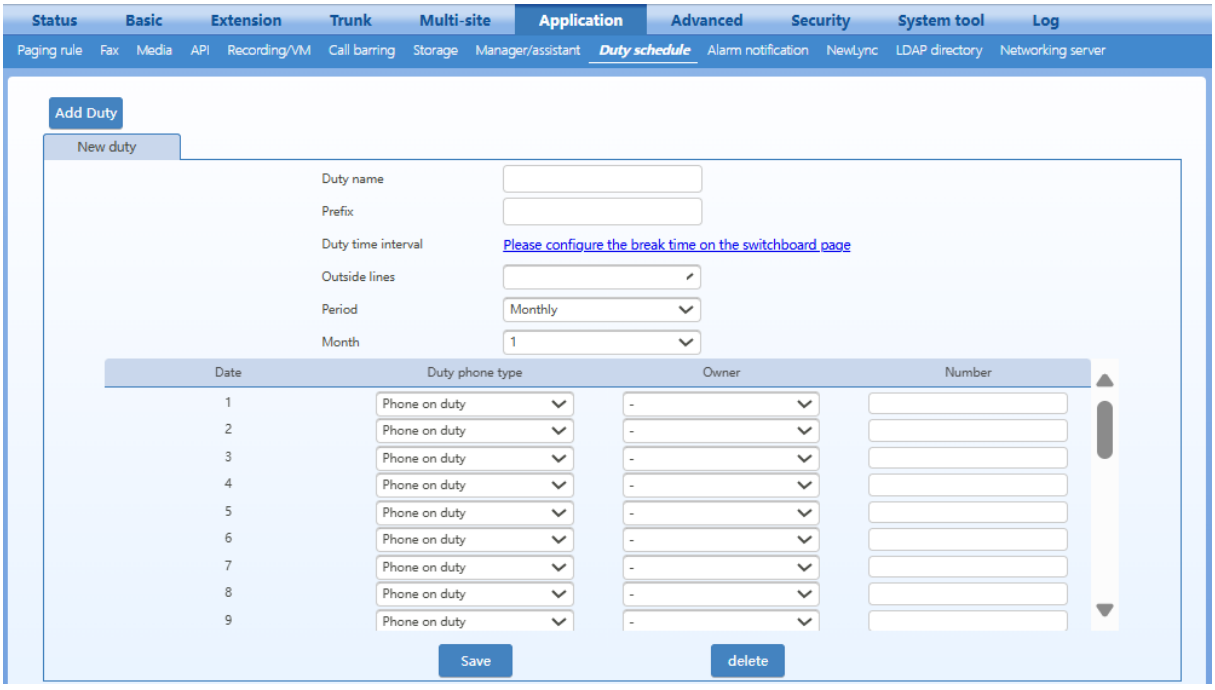


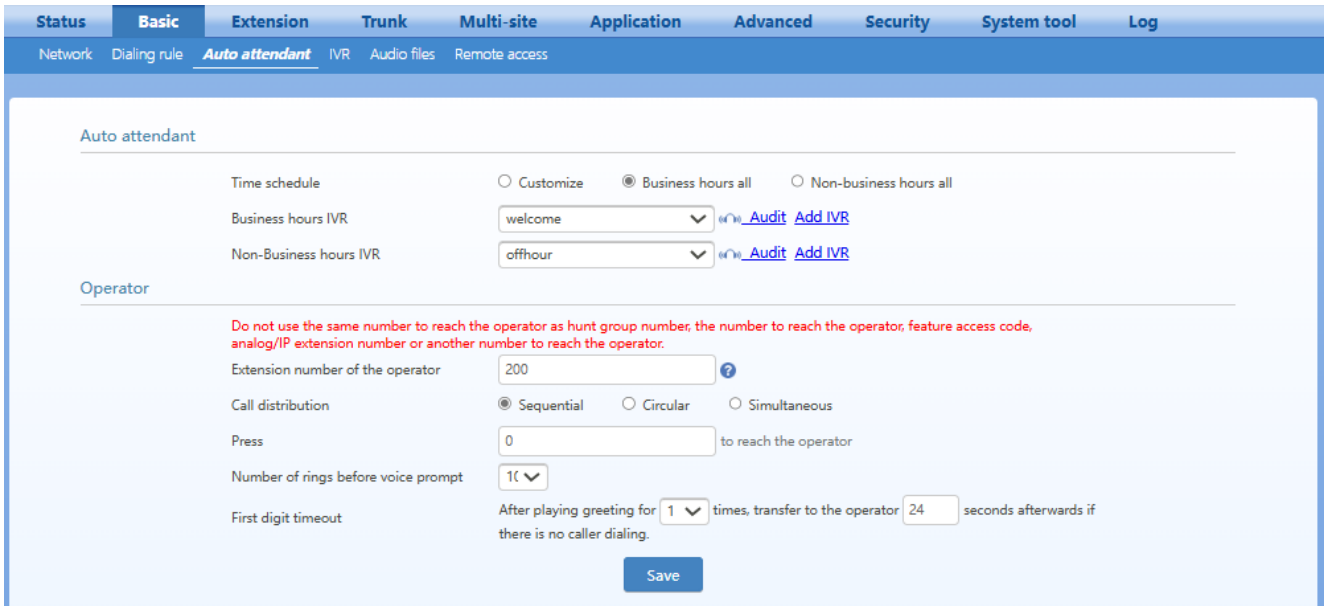
Table 2-34 Description of duty roster parameters

Item	Definition
Prefix	Used to specify the prefix of the outgoing number that needs to be set on duty to help the system recognize the matched incoming number.
Duty period	Set up specific time slots for the duty officer to answer outgoing calls. This setting allows the administrator to configure different duty officers or phone numbers for different time periods, thus automating duty management.
External line	Used to select or enter an outside line with duty requirements.
Cyclicality	Periodicity with which the duty roster is in effect: weekly or monthly. To select the week, you need to check the day of the week under the date, and to select the month date, you need to fill in the number of the month after the date.
Dates	Date used to configure the effective date of the on-call program
Months	Used to configure the month in which the on-call program is in effect
Type of duty call	Cell Phone: When "Cell Phone" is selected as the duty phone type, it means that the number of the duty officer to answer the outgoing call is a cell phone number. Extension: When "Extension" is selected, it means that incoming calls will be answered at the specified extension number. Networking Number: When "Networking Number" is selected, it means that the incoming call from outside line will be forwarded to the number of other devices in the network with the device. Duty number: When "Duty number" is selected, it indicates the dedicated phone number of the duty officer.
Person on duty	Employee or staff member responsible for answering outgoing calls during a specific time period.
Duty phone number	Phone number to answer an outgoing call during a specified time period.

Step 2 Configure specific duty schemes > Configure individual time periods. When configuring a time period that is not a full day, just specify the starting time. See 2.1 Automated Attendant for details.

 Copyright © Redstone Systems, Inc

Figure 2-69 Automated Attendant Interface



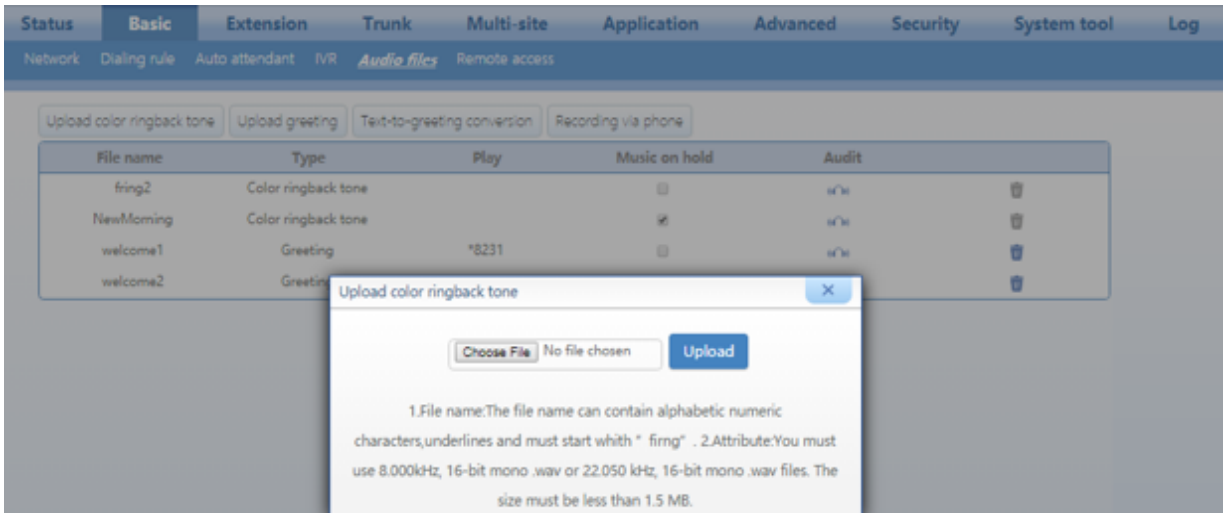
Step 3 Save Settings

2.9.3 Use of color ringtones

Step 1 Basic Settings>Voice Management, click Upload Ringtone to browse and upload the ringtone voice file. 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 of the uploaded voice file must be "fring+number", e.g. fring1, in wav format, and no more than 1.5MB in size. 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.

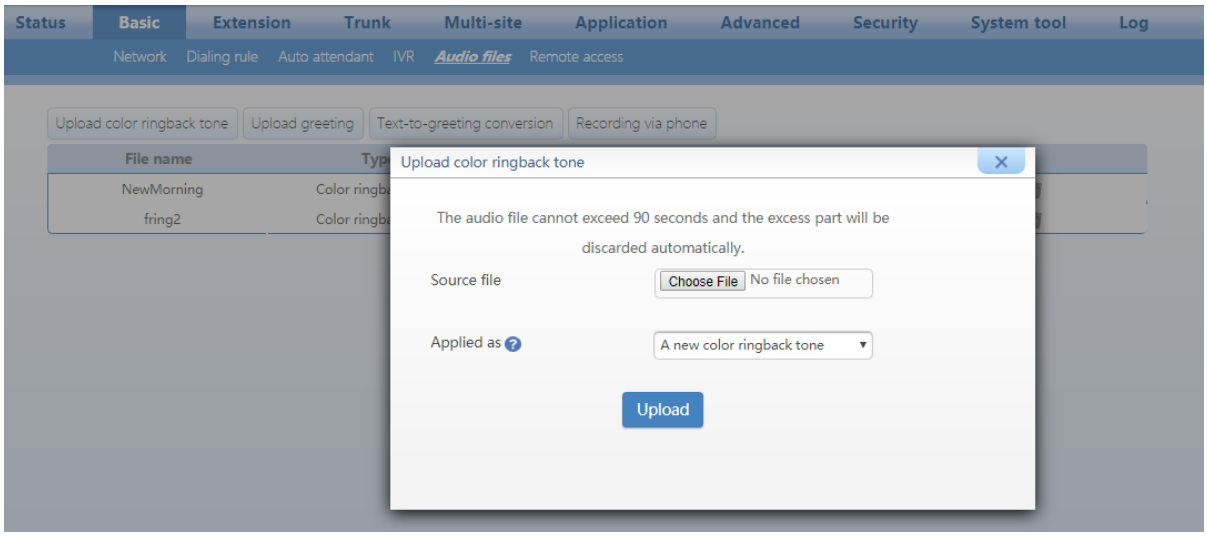
Figure 2-70 Color Ringtone File Upload Configuration Interface



The above methods have more requirements for uploading files, therefore, we recommend

 Copyright © Redstone Systems, Inc

you to download the "Wind Sound" software according to the prompts in the voice managementpage, and then upload the color ringtone files, at this time, the uploaded files only need to be one of the formats of MP3, WAV, M4A, WMA, AAC, OGG, AMR, 3GPP. The operation is shown below, at this point please make sure to open the page with Firefox or Google Chrome.



Step 2 Click Extension > Analog Extension (or IP Extension)> Settings to set the desired color ringtone for the extension.

Click to try out the colorful ringtones.

Step 3 Click Save.

Color ringtone voice files can also be used to set up background music, as detailed in the 02.9.4 Background music.

2.9.4 Background music

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 New Morning, and users can also upload their own voice files.

The device's color ringtone voice file and background music voice file can be common, after uploading the customized voice file, the steps for setting the background music are as follows:

Step 1 Go to Basic >Audio files, check the voice files that need to be set as background music and confirm to save.

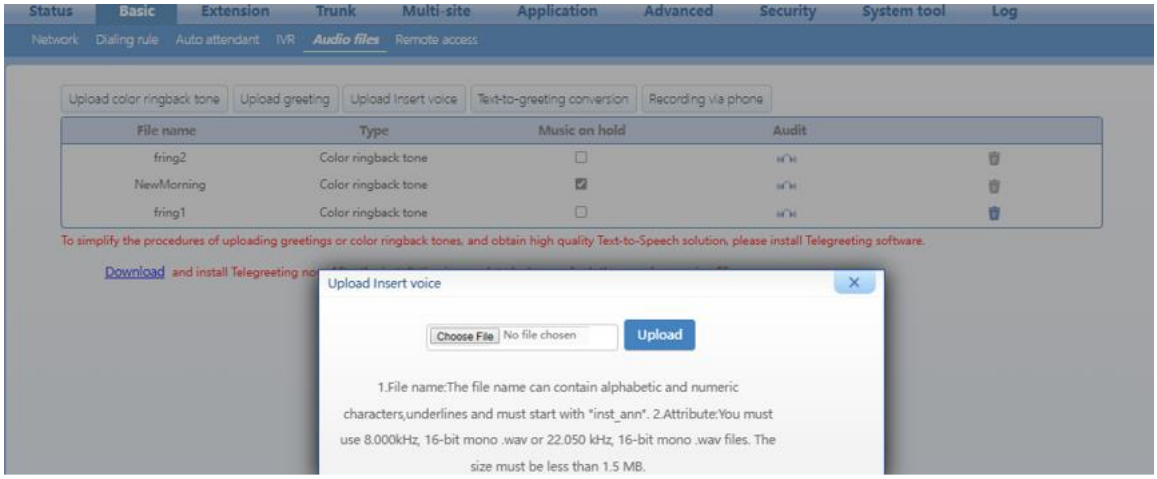
Click Audition to try the audio.

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

 Copyright © Redstone Systems, Inc

2.9.5 Uploading Interpolated Voice

Figure 2-71 Background Music Configuration Interface



In Basic Settings > Voice Management, upload the Insert Voice button feature. This function is used to upload the interpolated voice file, click the button to select the file for uploading, when the file is uploaded, it should meet the following requirements:

1. File name: must consist of letters, numbers and underscores and must begin with "inst_ann".

2. File attributes: must be 8.000 kHz, 16-bit or 22.050 kHz, 16-bitmono .wav files.

3. File size: The file size must not exceed 1.5MB.

After the upload is complete, you can use the inserted voice file to make the relevant settings.

2.9.6 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, which keeps it running when the device is powered off.

Click System Tools>System Time to configure the time server.

 Copyright © Redstone Systems, Inc

Figure 2-72 System Time Configuration Interface

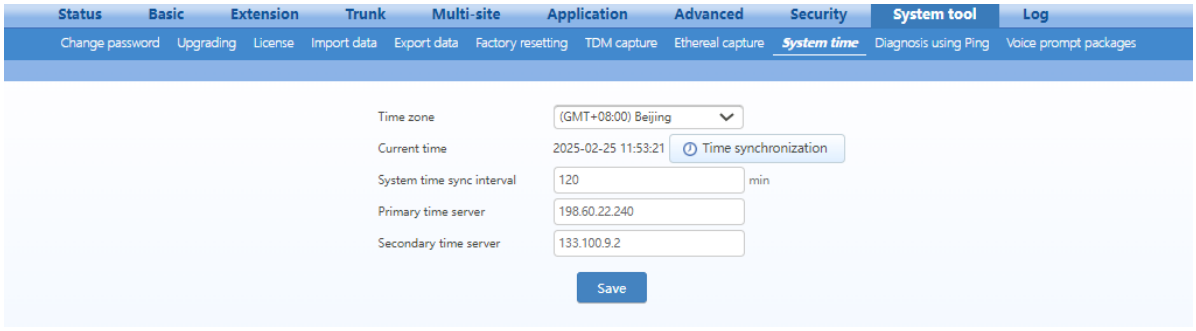


Table 2-35 Description of system time parameters

Item	Definition
Time zone	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.
System time sync interval	The period in minutes for the device to synchronize with the network time server, the default is 120 minutes.
Primary time server	Enter the preferred time server IP address here. There is no default value for this item.
Secondary time server	Enter the alternate time server IP address here. There is no default value for this item.

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.

 Copyright © Redstone Systems, Inc

2.9.7 Encryption

Go to Security >Encryption to open this screen.

Figure 2-73 Encryption Interface

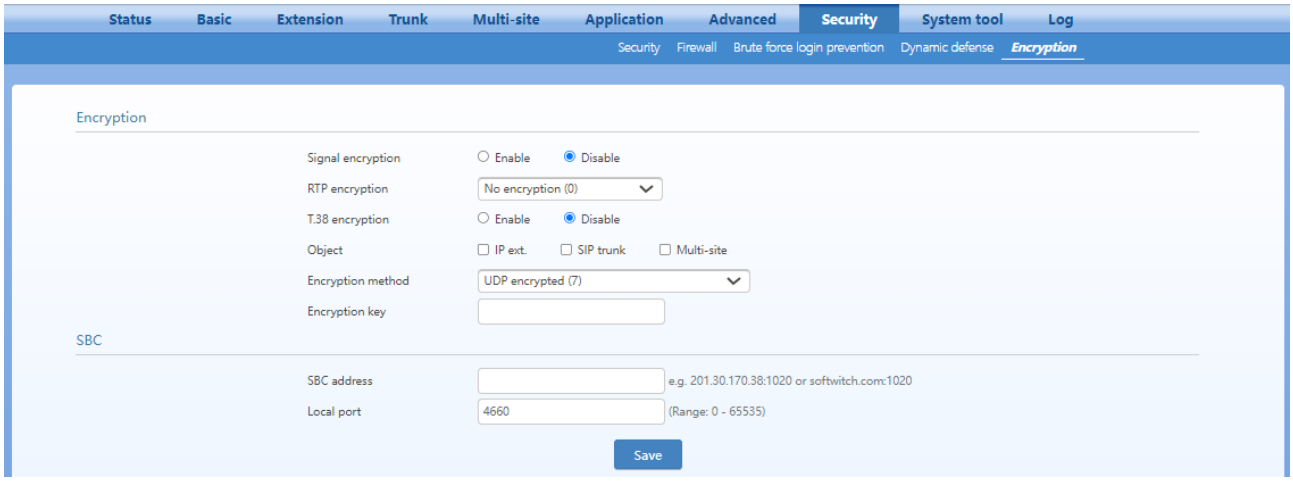


Table 2-36 Description of encryption parameters

Item	Definition
Signal encryption	Enables/disables signaling encryption. Default off.
RTP 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 encryption	Select whether or not to encrypt T.38 fax media stream packets, the default value is not selected.
Object	Select the encrypted object. Encrypted objects are divided into two categories: • Internally: IP extensions and networking. If the device turns on the encryption function internally, it is necessary for the terminal to support encryption, otherwise the terminal will not work. • External: SIP external line. Choose whether to encrypt or not according to the needs of the SIP server.

 Copyright © Redstone Systems, Inc

Item	Definition
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) • Specialized encryption in conjunction with CWNS softswitch (8) • Using UDP protocol with RC4 encryption algorithm (10) • Encryption in conjunction with Sentry and polylink products (14) • Special encryption with 263 softswitch (Word Reverse) (16) • Special encryption in conjunction with 263 Softswitch (Word Exchange) (17) • Special encryption (Byte Reverse) in conjunction with 263 softswitch (18) • Special encryption in conjunction with 263 softswitch (Byte Exchange) (19) • Special encryption in conjunction with Nanjing Kunshi VOS system (20) • Special encryption in conjunction with the Beijing Tianzhou communication system (21) The encryption method corresponding to different softswitch platforms can be selected as needed.
Encryption key	from the operator or system administrator.
Sbc	When using the encryption method numbered (2) (3) (6) (7), it is necessary to use it with the Swift-Time SBC product.
SBC address	Set the IP address and port number of the border proxy server. The address and port number are separated by ":". The proxy server address can be in the form of an IP address or in the form of a domain name, depending on the user's requirements. A complete and valid configuration is for example: 201.30.170.38:1020 or softswitch.com:1020. When using a domain name form of address, you need to configure a domain name resolution server in theBasic Configuration > 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 user name, required when the encryption method is "special encryption (20) with Nanjing Kunshi VOS system".
Password	VOS encryption key password is required when the encryption method is "Special encryption (20) with Nanjing Kunshi VOS system".

 Copyright © Redstone Systems, Inc

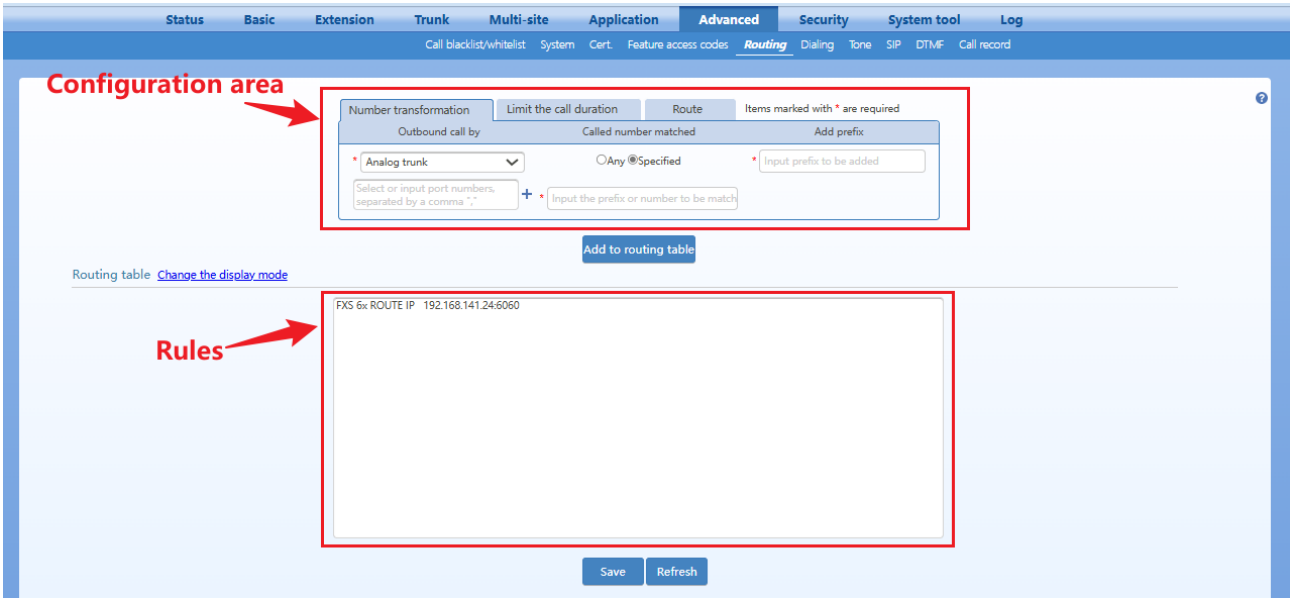
2.9.8 Routing Tables

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 Definition are given below:

Number conversion

Figure 2-74 Routing Table Configuration Interface of Number Transformation



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

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

Note: The outside line type is indicated by FXS and FXO, FXS means outgoing via IP outside line and FXO means outgoing via analog outside line.

 Copyright © Redstone Systems, Inc

Examples:

- Analog outbound call, called add prefix 17909

  FXO *X* ADD *17909*

- Analog outgoing domestic long-distance calls, called add prefix 17909

  FXO *0* ADD *17909*

- Analog outgoing international calls from outside line, called add prefix 17909

  FXO *FXO* ADD *17909*

- Specific analog outside calls to specific called (e.g., analog outside 1, 2, 3, 4, 6 call out to called numbers beginning with 9), add prefix 17909

  FXO [1-4, 6] *9* ADD *17909*

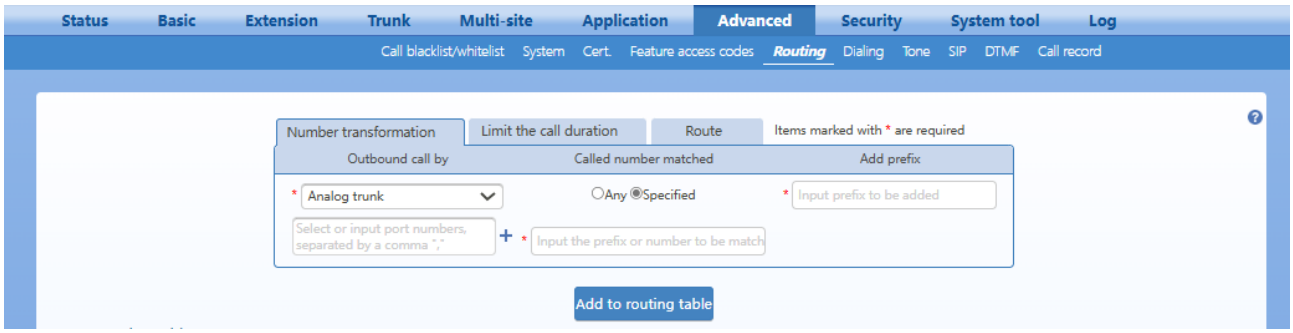
- IP outbound call, called add prefix 17909

  FXS *X* ADD *17909*

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

  FXS *10* ADD *17909*

2. Interface Configuration Rules



 Copyright © Redstone Systems, Inc

Item	Definition
Call from	Select Analog Outside Line or IP Outside Line, and then tap the plus sign after the input box below to specify the specific line.
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.

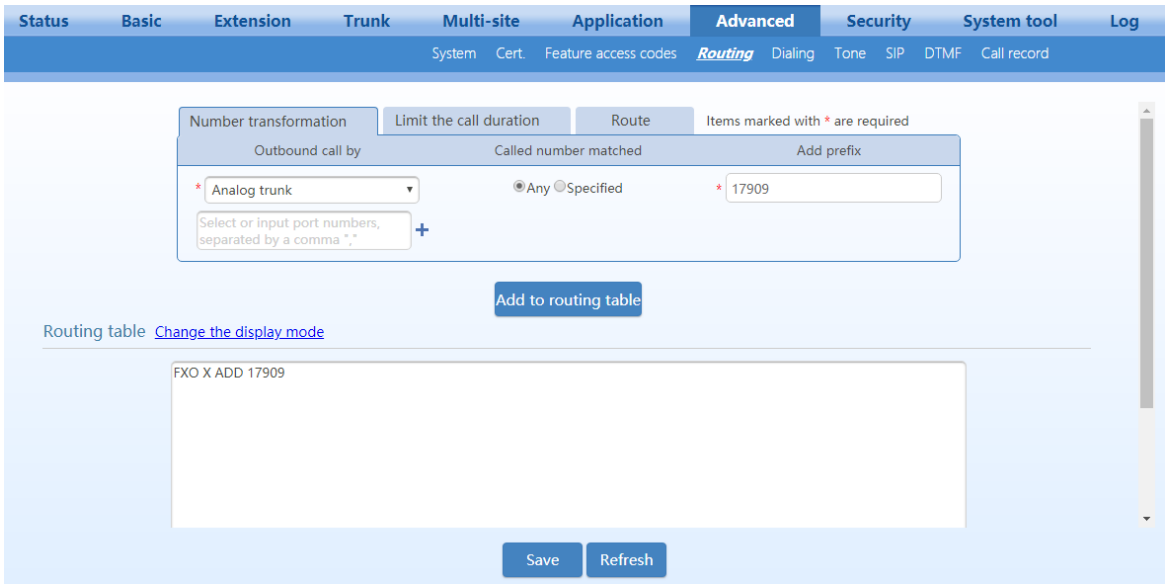
Example: simulate an outgoing call from an outside line by adding the prefix 17909 to the called.

Configuration method:

Select "Analog Outgoing Line" for the outgoing line, select any number for the called number, and enter "17909" in the number prefix field.

Click Add to Routing Table.

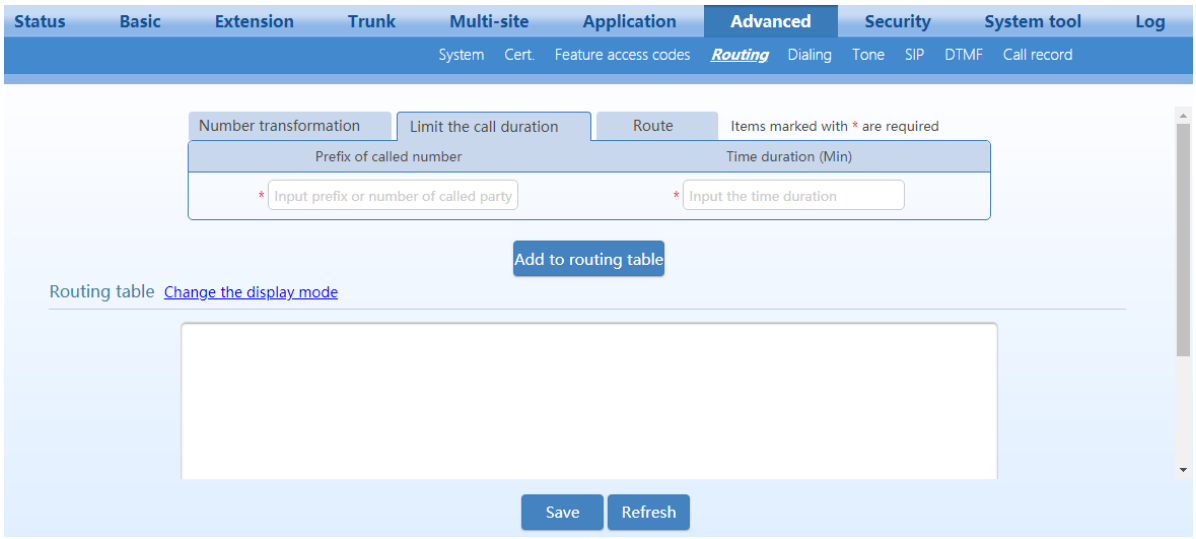
The final routing rule is generated: FXO *X* ADD *17909, which appears in the routing table below.*



 Copyright © Redstone Systems, Inc

Outgoing time limit

Figure 2-75 Routing Table Configuration Interface of Call Duration Restriction



1. Command writing rules: FXS *Called prefix* TIME*Individual call duration limit/total duration/type/remaining duration (where the remaining duration is the result of the system calculation and does 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:

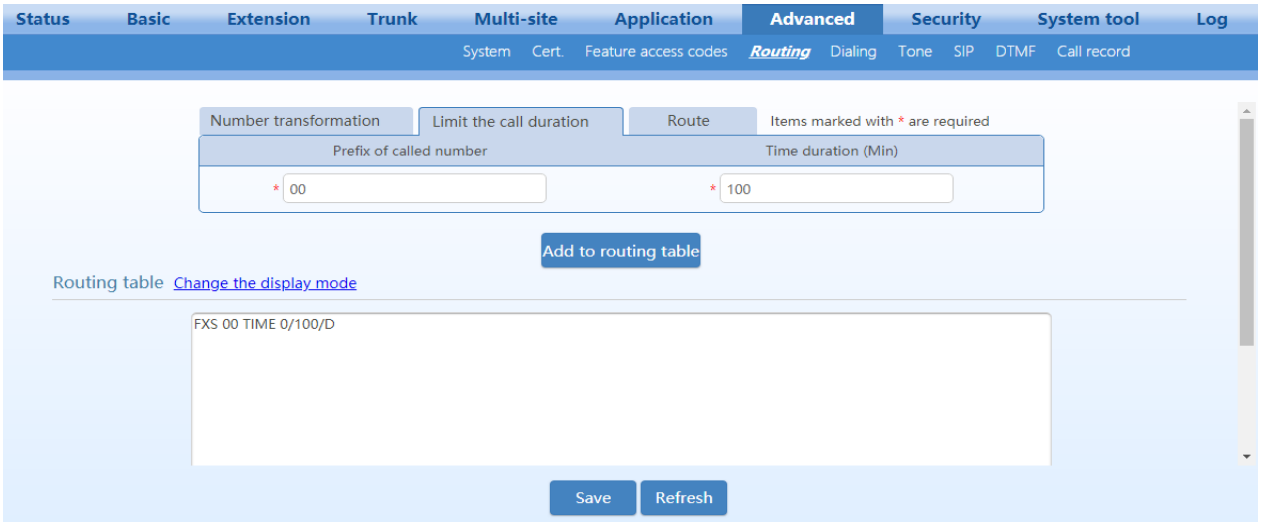
- Calls to a specified caller (e.g., international calls, i.e., called numbers beginning with 00), with a limit of 100 minutes per day, unlimited for individual calls

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

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

 Copyright © Redstone Systems, Inc

2. Interface Configuration Rules



Item	Definition
Called prefix	The called number of the call matches this prefix, then the call limits the call duration according to the rules.
Time 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.

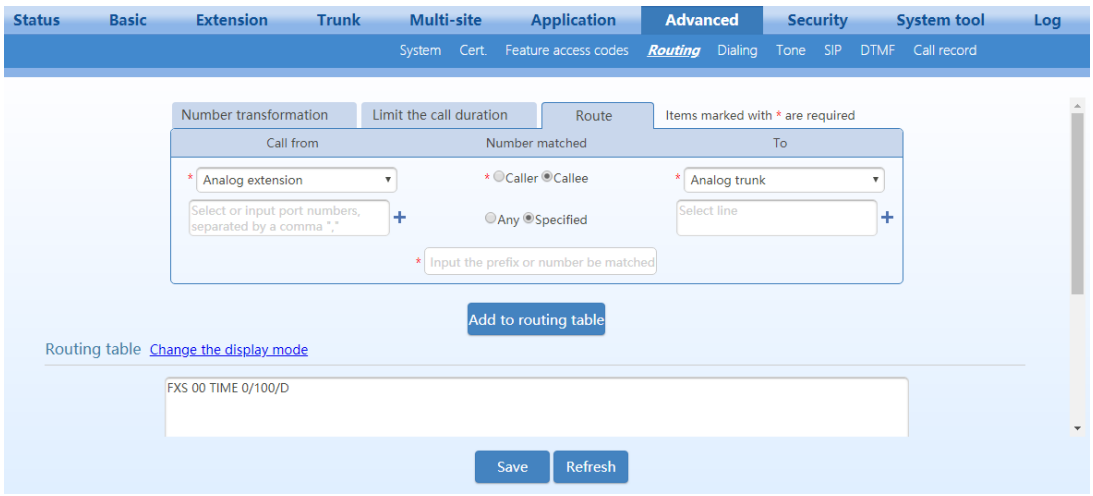
Example: The total call duration for international calls is limited to 100 minutes.

Configuration method:

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

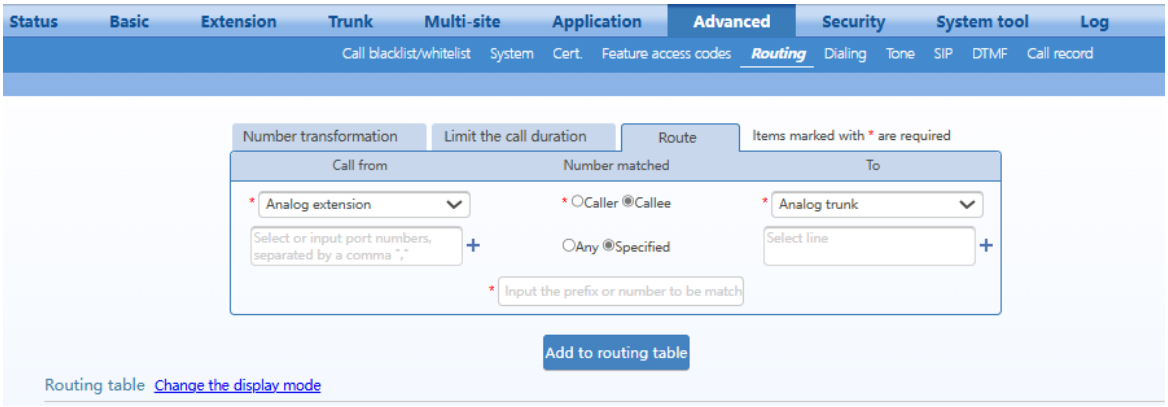
Click Add to Routing Table.

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



 Copyright © Redstone Systems, Inc

Directional Routing



1. Command writing rule: FXS *Called prefix* ROUTE *Route destination*

This rule is used to specify the routing destination for outgoing calls that match the *called prefix*, and this function needs to be used with the outgoing call rule to set the route selection method to "Route" mode.

Note: The directional routing rule starts with "FXS" regardless of whether the originating extension is an analog or IP extension. The routing destination can be FXO (for analog outbound), IPT (for IP outbound), or IP (for specific IP address).

Examples:

- The call is designated to be called (e.g., beginning with 6120) and is sent to the FXO port in the down-selected manner; when the FXO1 port is busy, the FXO2 port is selected

  FXS *6120* ROUTE *FXO 1-2*

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

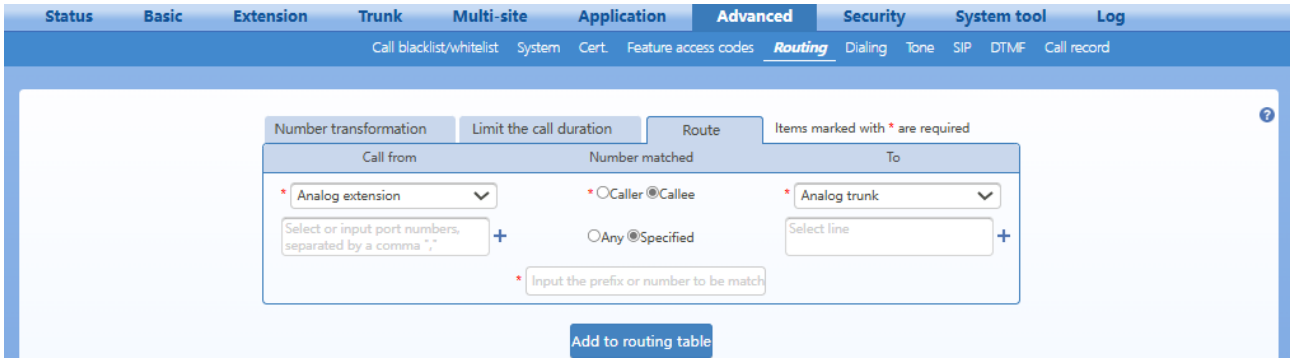
  FXS *6120* ROUTE *IPT 1~6*

 Copyright © Redstone Systems, Inc

- 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



Item	Definition
Call from	A call originating from a specified extension is indicated by selecting the analog extension or IP extension first, and then specifying the specific extension by placing a plus sign to the right of the input box below.
Number match	You can match the calling number or the called number. If you select prefix in the input box below the specified number, the prefix will be used to match the calling or the called number, and after matching, you can execute the routing rule.
To	Select the outgoing line, analog outgoing, IP outgoing, IP address or POS/Modem pass-through, and you can also click the plus sign to select a specific line.

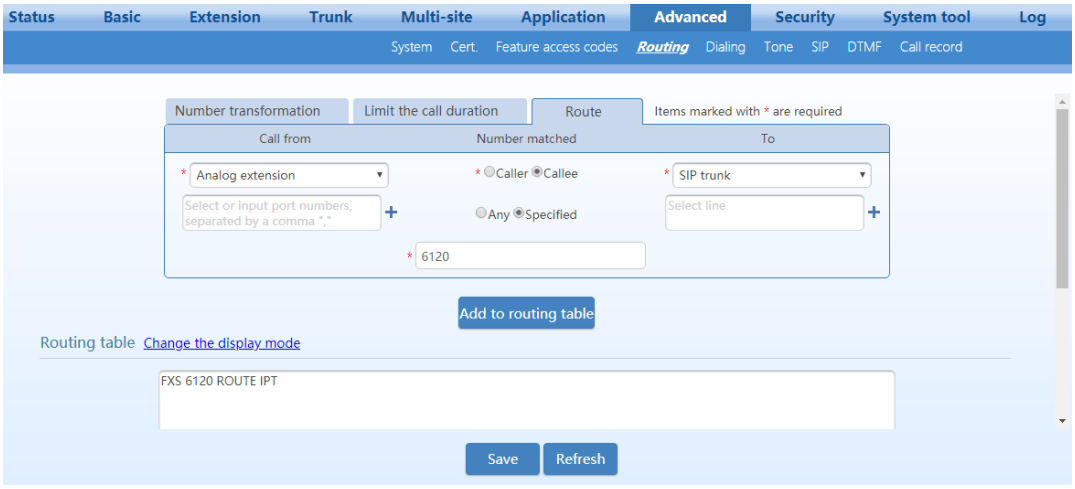
Example: An analog extension calls a specified called (e.g., beginning with 6120), which is sent to an IP outside line in accordance with the down-select method.

Configuration method:

Select "Analog Extension" for Call Source, select "Called" and "Assigned Number" for Number Matching, and enter "6120" in the input box below. "

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

 Copyright © Redstone Systems, Inc

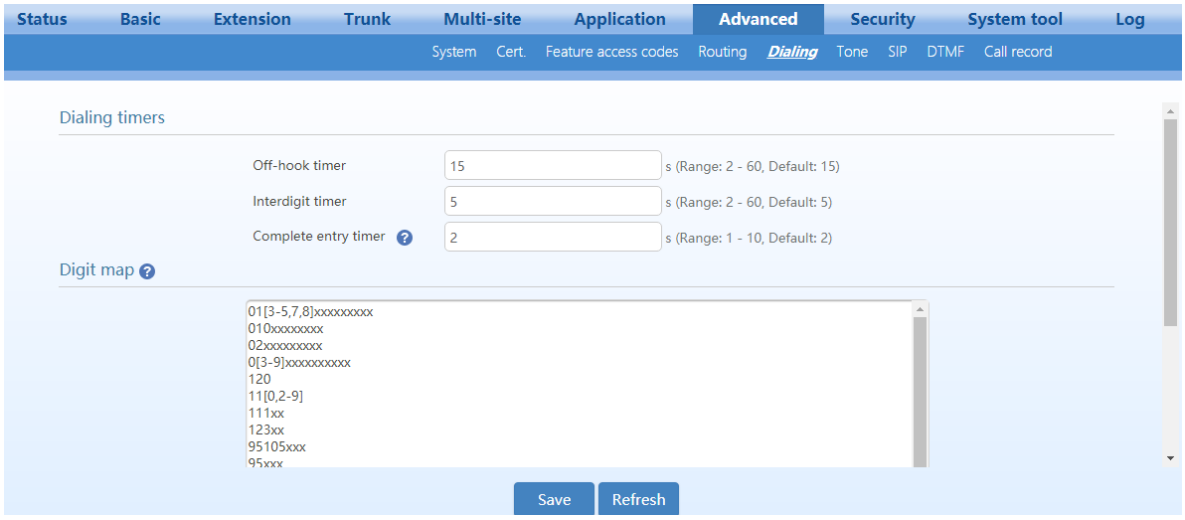


2.9.9 Dial Detection and Number Bitmap

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 >Dialing Detection to set rules related to the number bitmap.

Figure 2-76 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

 Copyright © Redstone Systems, Inc

following are the basic symbols used in the matching rules and Definition for their use.

Table 2-37 Explanation of the rules of the common numbered digit map

Number plan	Definition
Off-hook timer	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.
Interdigit timer	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.
Complete entry timer	Used in conjunction with the "XXXXXXXXXXXXX.T" rule in the numbered bitmap. The default is 2 seconds.
0-9, *, #	Match specific DTMF signals (corresponding to the dialing keys on the phone).
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.

 Copyright © Redstone Systems, Inc

2.9.10 Call Progress Tone

Go to Advanced Settings>Tones and set tones such as dial tone, busy tone, ringback tone, etc. by country or customize them.

Figure 2-77 Tone Setting Interface

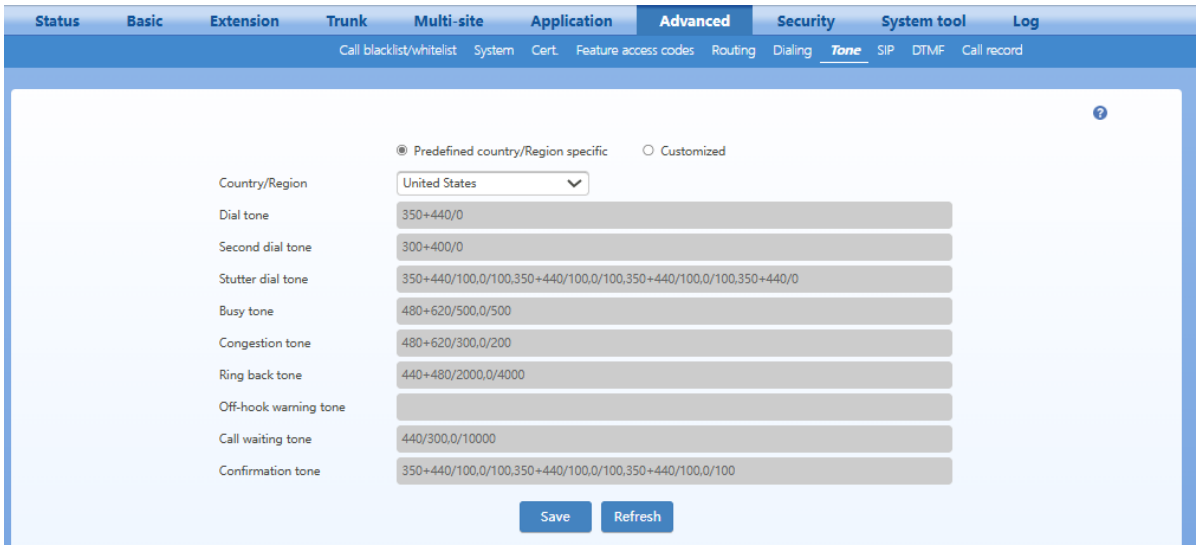


Table 2-38 Description of Beep Parameters

Item	Definition
Tones	System Preset: Select the country/region built into the system. Customization: Users can define the following call tone parameters by themselves.
Country/area	Sets the signal tone standard of the country used by the device, the default value is "China". In addition the following national and regional signal tone standards are available in the device: China, United States, Singapore, Israel, Malaysia, Indonesia, United Arab Emirates, Australia, Zimbabwe, France, Italy, Germany, Mexico, Chile, Russia, Japan, Korea, Hong Kong, Taiwan, India, Sudan, Iran, Algeria, Pakistan, Philippines, Kazakhstan, Turkey, Argentina.
Dial tone	Off-hook dial tone.
Second dial tone	For secondary dialing applications.
Stutter dial tone	Used to alert the extension user of the following conditions: that Do Not Disturb is turned on or Unconditional Call Forwarding is turned on, or that there is a new voice message.
Busy tone	Used for busy tone alerts.
Congestion tone/reorder tone	Used for alerts when you cannot get through due to resource constraints.
Ring-back tone	An alert tone to the calling party when ringing.
Off-hook warning tone	Alerts the user that the phone is in the off-hook non-dialing state.

 Copyright © Redstone Systems, Inc

Item	Definition
Call waiting tone	Alerts the user's phone in a call that there is a new incoming call.
Confirmation tone	Used for confirmation prompts after entering a function key.

Table 2-39 Examples of customized tone rules

give an example	Definition
350+440	Dual frequency tones consisting of 350 and 440 Hz.
480+620/500, 0/500	A dual-band tone consisting of 480+620 Hz is played repeatedly in 500 ms play 500 ms stop. Note:0/500 means 500 milliseconds of silence.
440/300, 0/10,000, 440/300, 0/10,000	440 Hz single-frequency tone, repeated 2 times at 300 ms playback with a 10-second stop.
950/333, 1400/333, 1800/333, 0/1000	Play 333 milliseconds at 950 Hz, 333 milliseconds at 1400 Hz, 333 milliseconds at 1800 Hz, mute for 1 second, repeat.

2.9.11 SIP Compatibility

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

Figure 2-78 SIP Compatibility Interface

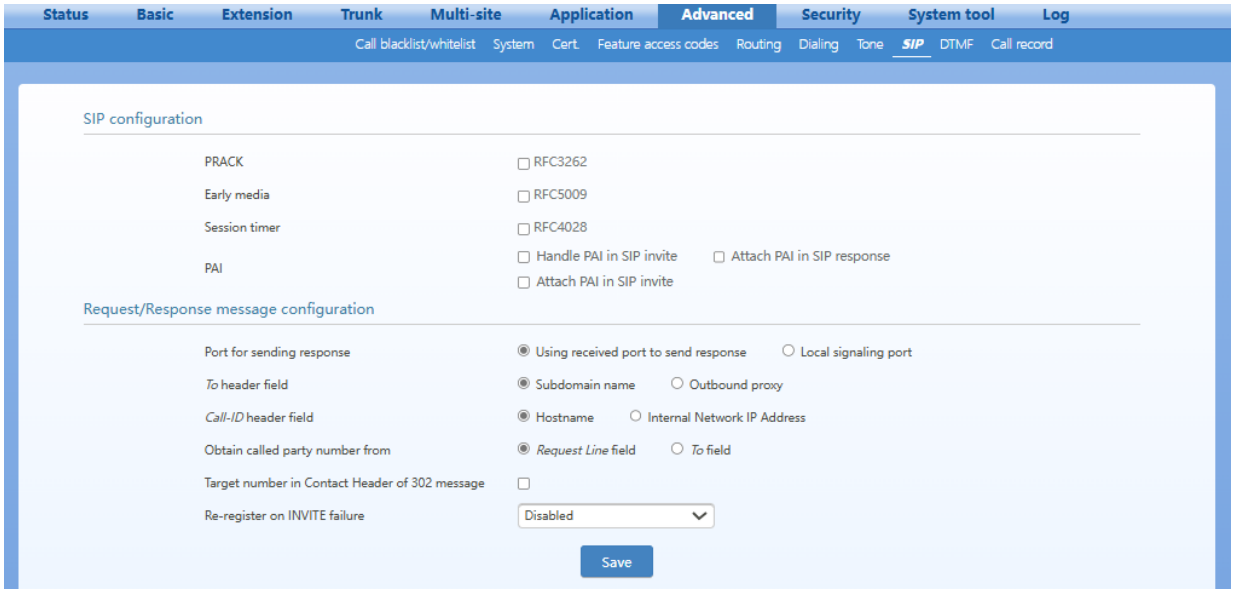


Table 2-40 SIP Compatibility Parameter Description

Item	Definition
PRACK	Open RFC3262, PRACK. The system default is unchecked.
Early Media	Open RFC5009. The system default is unchecked.

 Copyright © Redstone Systems, Inc

Item	Definition
Media Stream Direction Attributes	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. Note: This can be configured when Early Mediais checked.
Session timer	Session Refresh (RFC4028) uses periodic re-INVITE or UPDATE requests and corresponding response messages during a call to determine if the call is "alive" so that resources can be released in a timely manner. When the sender of a session refresh request (the refresher) does not receive a response or the receiver of the request does not receive a refresh request within the refresh cycle, it assumes that the other party does not exist, ends the call, and releases the resources. The refresher and refresh period are determined by negotiation between the parties involved in the call, including both parties to the call and the various agents in transit. 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 turns off the word refresh function 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.
Session 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 timer	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.
Selecting the receiving port for response	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".

 Copyright © Redstone Systems, Inc

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

2.9.12 DTMF

Go to Advanced Settings> DTMF to configure DTMF information.

Figure 2-79 DTMF Interface

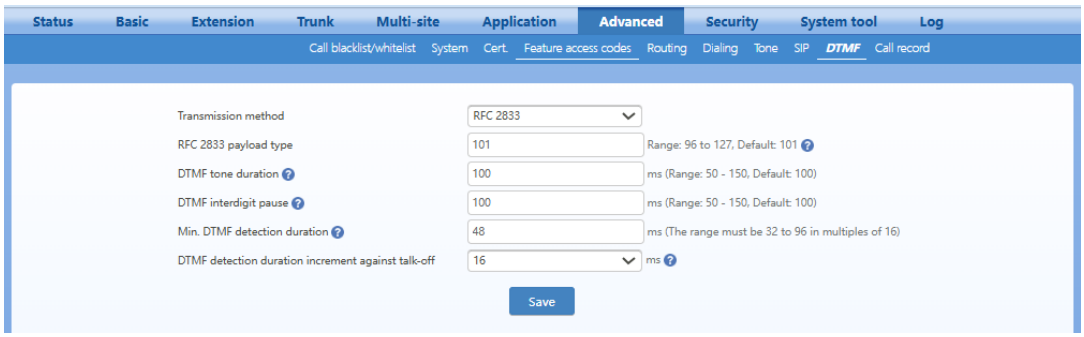


Table 2-41 DTMF Parameter Description

Item	Definition
Transmission method	The transmission methods of DTMF signals supported by the REX are RFC2833, Transmission, and SIP INFO, and the default is RFC2833. • RFC 2833: Separates the DTMF signal from the voice path and transmits it to the platform via RTP packets in RFC2833 format; • Transmission: The DTMF signal is transmitted to the platform along with the voice path; • SIP INFO: Separates the DTMF signal from the voice path and transmits it to the platform as a SIP signaling INFO message.

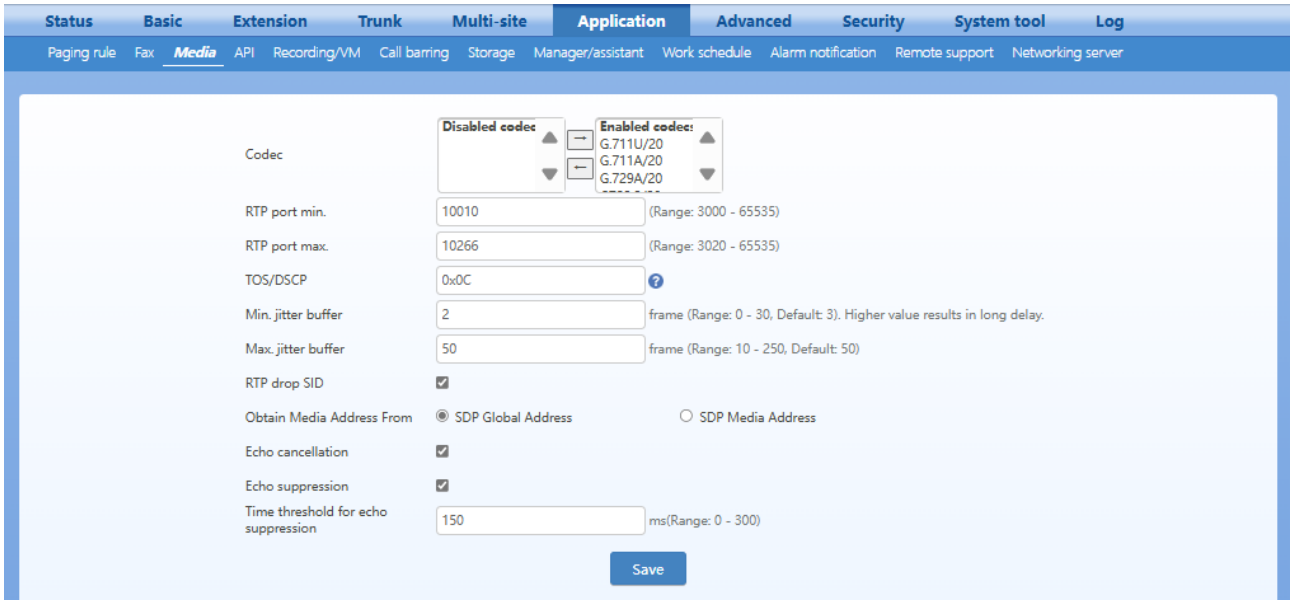
 Copyright © Redstone Systems, Inc

Item	Definition
RFC 2833 payload type	If RFC 2833 transmission method is selected, you need to configure the option, the value range is 96~127, and the default value is 101. Users should note when configuring this parameter that the value of this parameter and the value of 2833 packet type supported by the opposite end should be the same.
DTMF Tone duration	This parameter specifies the DTMF signal duration in milliseconds from the FXO port. The default value is 100 milliseconds. It should normally be set in the range of 50 ~ 150 ms.
DTMF Inderdigit pause	This parameter specifies the time in milliseconds between DTMF signals from the FXO port. The default value is 100 milliseconds. Typically, it should be set in the range of 50 ~ 150 ms.
Min. DTMF detection duration	Minimum duration of a valid DTMF signal. The valid range is 32 to 96 milliseconds and must be a multiple of 16, the default value is 48 milliseconds. The larger the setting, the stricter the test.
DTMF detection duration increment against talk-off	Takes a value in multiples of 16 in milliseconds. When the DTMF signal misdetection is serious, the value of this parameter can be increased.

2.9.13 Media

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

Figure 2-80 Media Configuration Interface



 Copyright © Redstone Systems, Inc

Table 2-42 Description of media parameters

Item	Definition
Codecs	The device supports multiple codecs: G.729A/20, G.711U/20, G.711A/20, G.722.2/20, G.722/20. This item can be configured with multiple encoding methods at the same time, separated by English commas. When multiple encoding methods are configured, 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. Default value 10010, value range 3000~65535, it is recommended to configure the value not less than 10000. Note: Each call will occupy both RTP and RTCP ports. For example, if the device has 4 user lines (or trunks), it needs to use 8 UDP ports.
RTP port Max	The maximum value of the transmit and receive ports for RTP. Default value 10266, value range 3020~65535. It is recommended that the configuration value is greater than or equal to "2 x number of lines + minimum value".
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 voice quality for IP calls.
Max. Jitter buffer	The RTP Jitter Buffer helps to overcome the effects of network jitter. This parameter configures the maximum number of RTP packets that can be retained in the buffer, and the default value is 2 frames. The range of values is 0 to 30 frames.
Min. Jitter buffer	The RTP Jitter Buffer helps to overcome the effects of network transmit jitter. This parameter configures the minimum 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.
RTP drop SID	Select to discard received RTP SID voice data frames. 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.
Obtain Media Address From	• 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).
Echo cancellation	Echo cancellation switch. Enabled by default.
Echo suppression	Echo Suppression Switch. Enabled by default.
Time threshold for echo suppression	Sets the echo suppression length threshold, range 0 to 300 milliseconds, default 150 milliseconds.

2.9.14 Call Records

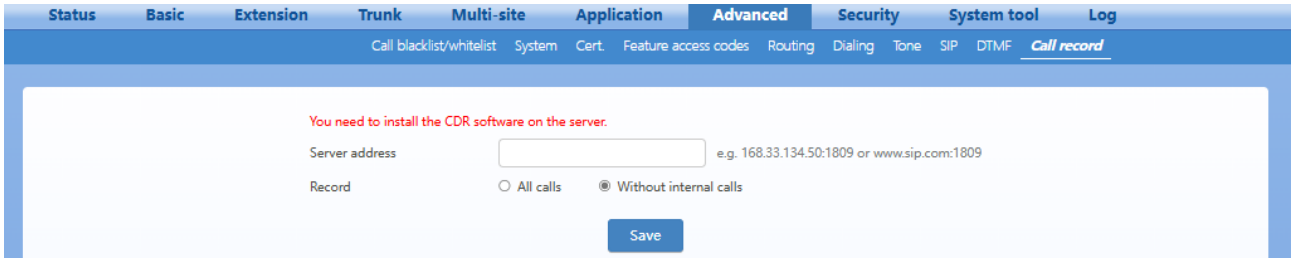
The device can provide a detailed record of each call, including the caller number, called number, call start and end time, etc.

 Copyright © Redstone Systems, Inc

Call records are sent from the device to an external server at the end of a call, and can be accessed and managed by managers through the Call Record Management (CDR) software pre-installed on the server.

Click Advanced >Call record to configure the call logging server address and port number, default port 1809.

Figure 2-81 Call Log Configuration Screen



2.9.15 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:

Step 1 Go to Application Services > API and fill in the API authentication address.

 Copyright © Redstone Systems, Inc

Figure 2-82 API Configuration Interface

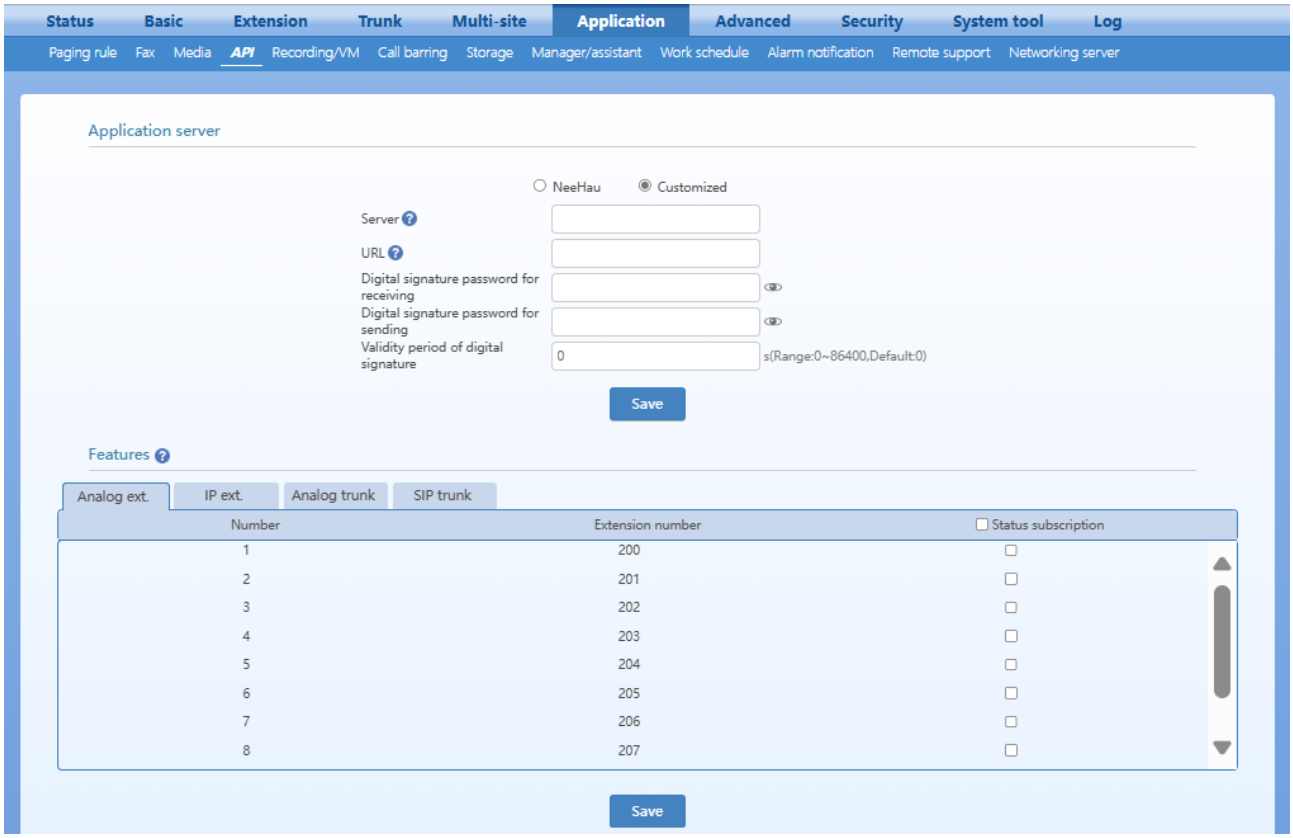


Table 2-43 API Interface Parameter Description

Item	Definition
NeeHau	Selecting Neehau means using Neehau Business Phone Assistant as the application server. No other application servers can be configured at this time. The REX1000 does not have Neehau option.
Serve	After selecting Customize, enter the third-party application server address and port number. The default value of 80 is used when the port number is not specified. The REX only recognizes API request messages from this IP address, and when the REX needs to proactively push API report messages to the application server, it also pushes to this address. Note: Turn off Neehau before you can configure this parameter.
Url	Enter the address (relative path) of the Web page used by the application server to receive device messages.
Digital signature password for receiving	The REX only receives API request messages from authenticated application servers. After configuring the REX digital authentication password, the key assigned on the application server needs to be consistent with the one configured here.
Digital signature password for sending	The REX can send API requests to the application server only after it has been authenticated by the application server. The digital authentication password configured here needs to be the same as the key configured on the application server.

 Copyright © Redstone Systems, Inc

Item	Definition
NeeHau	Selecting Neehau means using Neehau Business Phone Assistant as the application server. No other application servers can be configured at this time. The REX1000 does not have Neehau option.
Validity period of digital signature	Configured when digital signature authentication is used. The range of values is from 0 to 86400 seconds, and the default is 0 for permanent effect.

Step 2 Enable the API function for the extension/outside line.

Step 3 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.

2.9.16 Site attribution area digits

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

Figure 2-83 Attribution Area Bit Number Configuration Screen

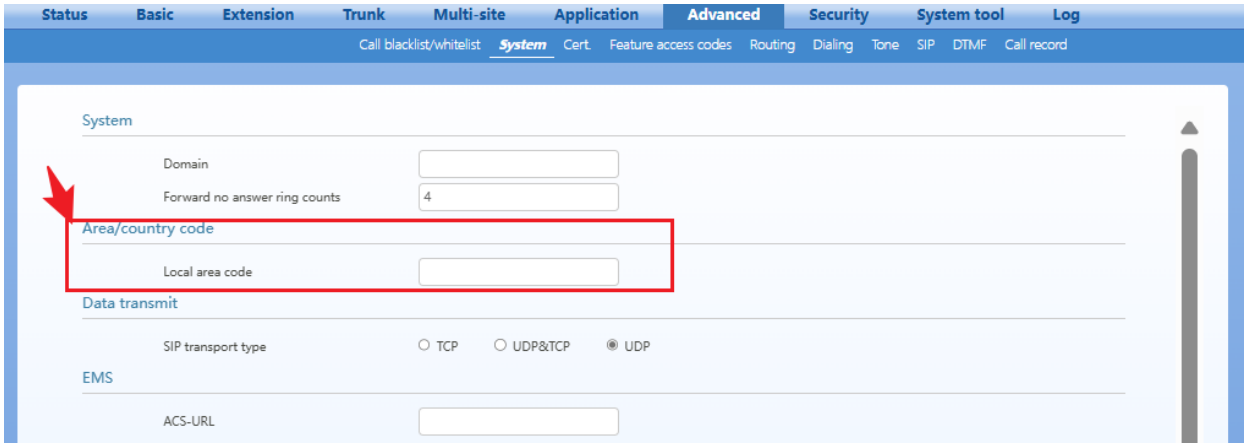


Table 2-44 Explanation of attributed area code parameters

Item	Definition
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.

 Copyright © Redstone Systems, Inc

2.9.17 SIP Transmission Method

Go to Advanced Settings>System to set the SIP transfer method.

Figure 2-84 SIP Transmission Mode Configuration Interface

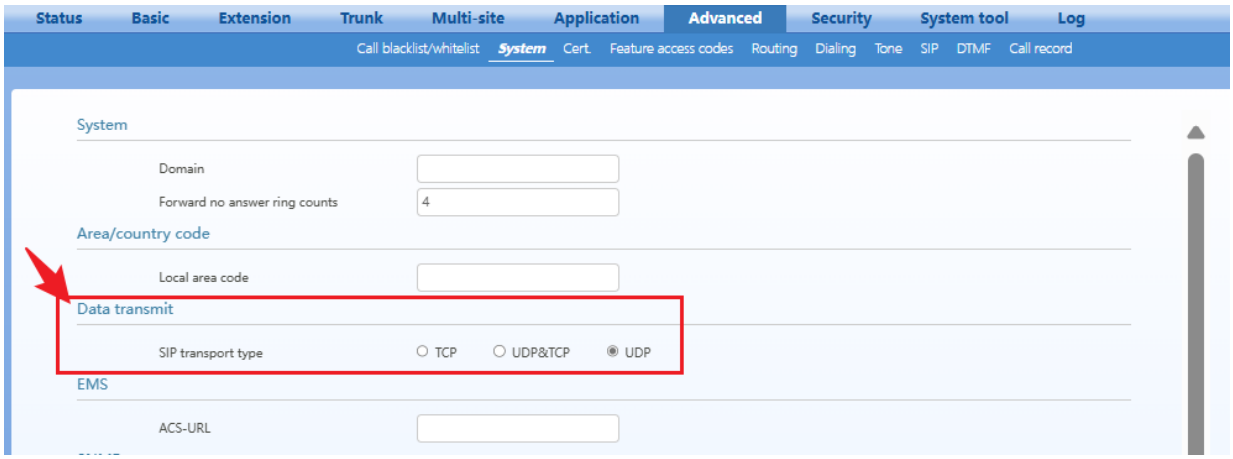


Table 2-45 SIP transmission method parameter description

Item	Definition
SIP transmission method	Select the transport layer protocol used to transmit SIP messages. UDP transmission method is selected by default, TCP or UDP&TCP can also be selected. The SIP transmission method must be consistent with the remote end.
TCP-based SIP local port	The SIP local port when using the TCP protocol for transmission.

2.9.18 Automated Management

Configuration automatic management function, can be through the automatic configuration server (ACS) for remote centralized management of the device configuration and firmware upgrade.

Go to Advanced Settings>System (REX1000) is to go to Advanced Settings>System, and select Auto Management for the network management platform method) to configure.

 Copyright © Redstone Systems, Inc

Figure 2-85 Automatic Management Configuration Interface

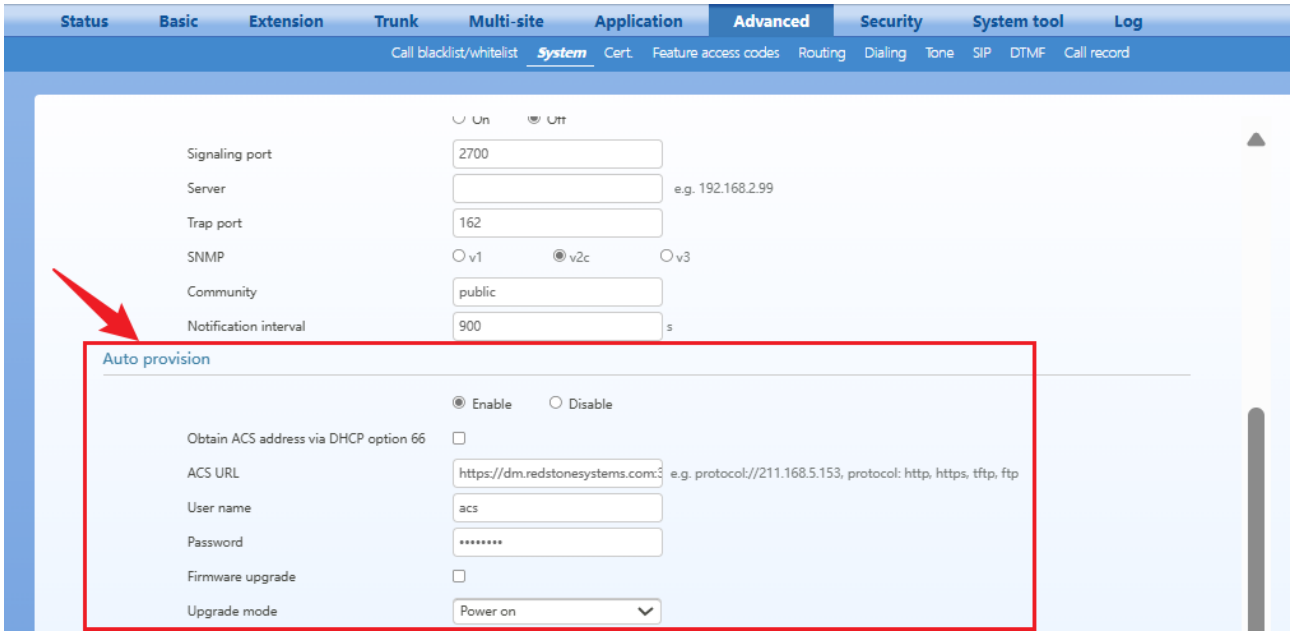


Table 2-46 Automatic management of parameters

Item	Definition
Obtain ACS address via DHCP option 66	Obtain the remote Automatic Management TFTP/HTTP/HTTPS server (ACS) address via DHCP option 66.
ACS URL	Manually configure the ACS address, which can be a TFTP, FTP, HTTP, or HTTPS server • TFTP server: tftp://ACS address • FTP server: ftp:// ACS address • HTTP server: http:// ACS address • HTTPS server: https://ACS address
User name	Enter the user name to access ACS. Note: If the ACS address is configured as a TFTP server then the user name and password entry boxes will not be displayed on the interface.
Password	Enter the password to access ACS.
Firmware Updates	Download the firmware upgrade package at the address of the firmware upgrade package in the downloaded configuration file, and the device automatically completes the software upgrade. Note: REX20/REX50/REX200/REX200-A/REX500 /REX1000 firmware can be a tar.gz file or img file.
Update mode	• Power-up: the device detects if there is configuration and firmware on the ACS that needs to be updated to the local unit only at power-up startup. • Power Up + Cycle: when the device powers up and starts up, it first detects whether there is any configuration and firmware on the ACS that needs to be updated to the local unit, and then it periodically detects it according to the set cycle value.

 Copyright © Redstone Systems, Inc

Item	Definition
Upgrade period	Configure the time interval for periodic auto-upgrade of the device when "Power On + Cycle" is configured. The default value is 3600 seconds. Value range: 5~86400 seconds.

2.9.19 TR069

Go to Advanced Settings>System to configure it.

Figure 2-86 TR069 Configuration Interface

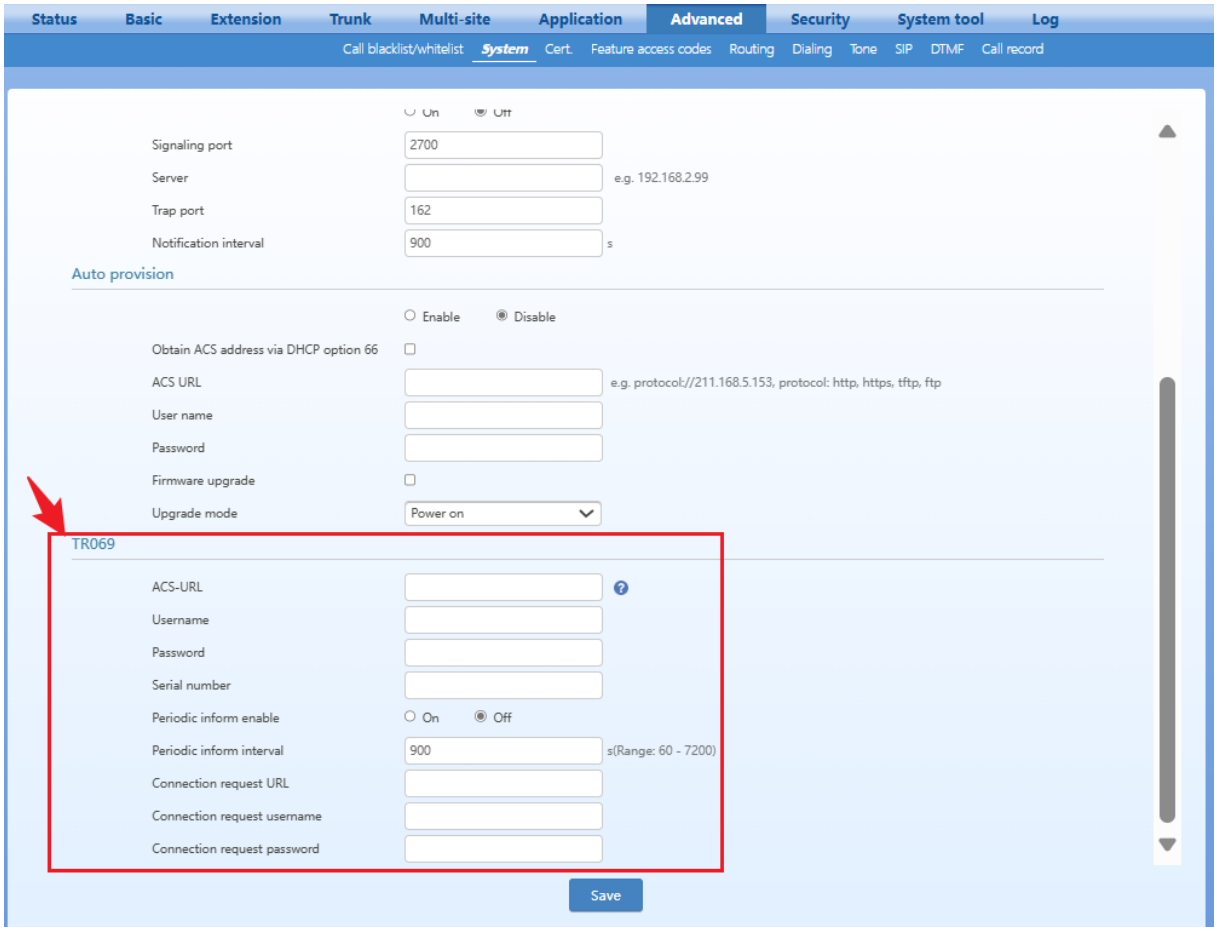


Table 2-47 TR069 Parameter Description

Item	Definition
ACS-URL	Set the URL of the webmaster server.
Username	Set the user name used for authentication with the network management server.
Password	Set the password used for authentication with the network management server.
Serial number	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.

 Copyright © Redstone Systems, Inc

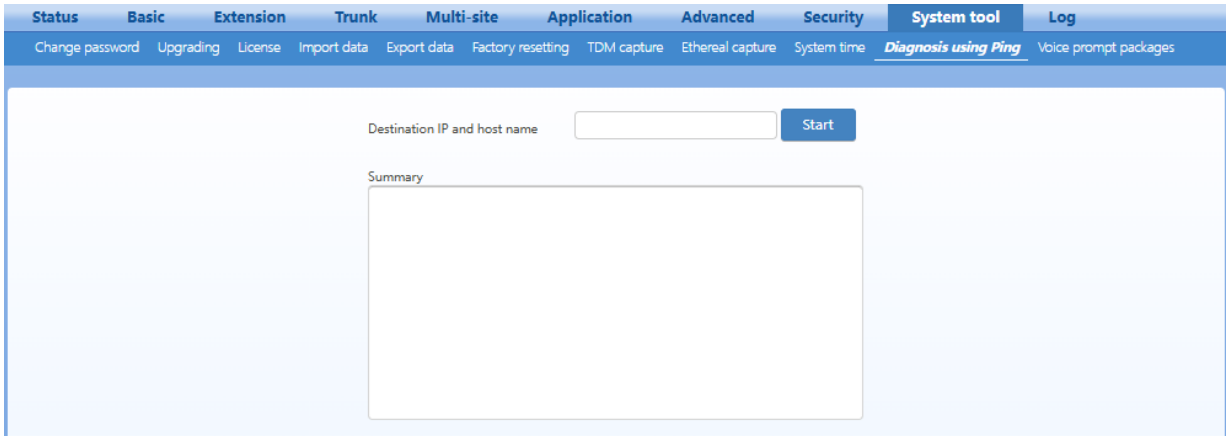
Item	Definition
Periodic inform enable	A switch that reports periodically to the network management server.
Periodic inform interval	The interval for reporting to the network management server.
Connection request URL	The address of the network management server's back-connected device. Generally generated automatically, you can also manually fill in the address of the device.
Connection request username	The account number of the network management server's back-connected device.
Connection request password	The password for the network management server to connect back to the device.

2.9.20 Ping Diagnostics (REX20/REX50)

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

Go to System Tools> 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.

Figure 2-87 Ping Diagnostic Interface



2.9.21 Voice package management

Each voice pack corresponds to one language and contains all system voice prompt files. For details, see Table 2-48.

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

Step 1 Click System Tools>Language Pack Managementto enter the configuration interface. The REX1000 requires an SD card to be inserted before this configuration interface is available.

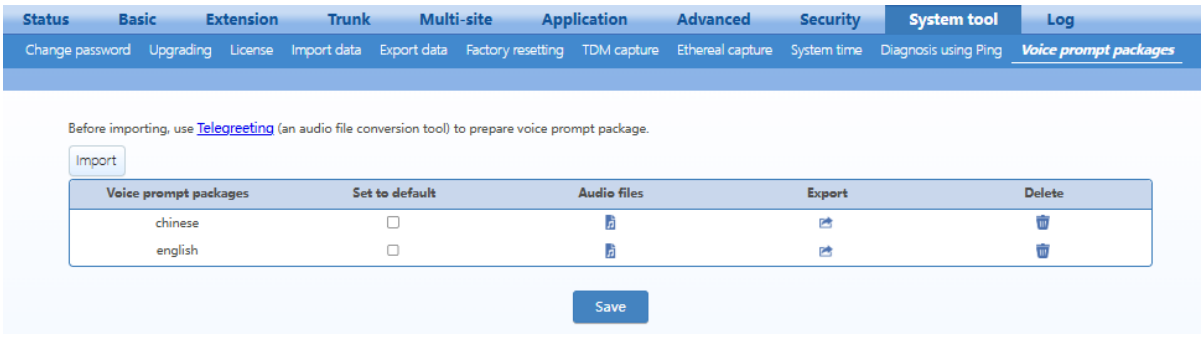
Step 2 Click Import Voice Pack to import a pre-made voice pack.

 Copyright © Redstone Systems, Inc

To create voice packs, you need to use the Wind Voice File Conversion Tool developed by Redstone, please refer to Wind Sound Voice File Conversion Tool User Guide The specific method can be found in the "Wind Voice File Conversion Tool User's Guide".

Step 3 Click the Set as default check box to set the system default voice pack.

Figure 2-88 Voice Pack Configuration Interface



Step 4 Click on the voice pack corresponding to , you can select individual voice files to upload for replacement as needed.

Figure 2-89 Voice Pack Configuration Interface

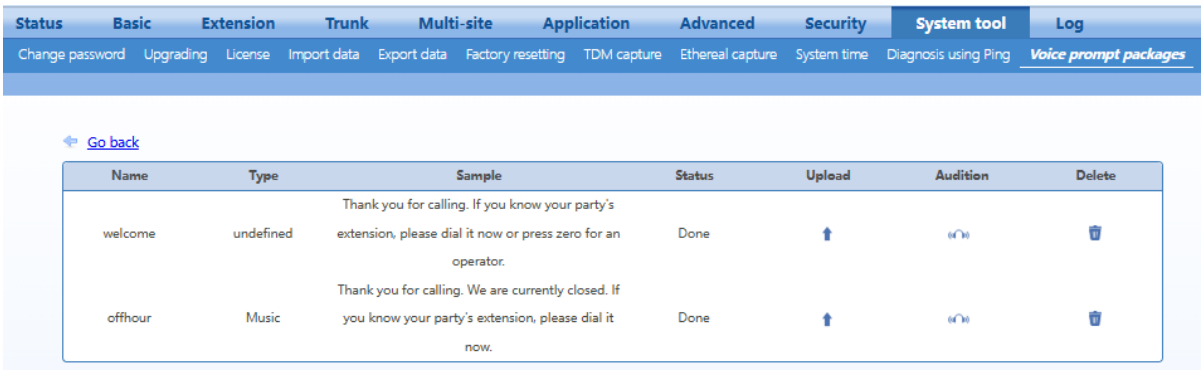


Table 2-48 System voice prompt file

filename	element
0_tip	Zero
1_tip	One
2_tip	Two
3_tip	Three
4_tip	Four
5_tip	Five
6_tip	Six
7_tip	Seven
8_tip	Eight
9_tip	Nine
account	Please enter the extension number, followed by the PIN.
block	You are not authorized to make this call. Please contact the administrator.

 Copyright © Redstone Systems, Inc

filename	element
busy	That line is busy. Enter another number now, or hold for an operator.
call waiting	Please hold. That line is busy, but your party has been notified of your call.
cancel	The feature is now deactivated.
confirm	The feature is now activated.
connect	Please hold while your call is transferred.
disable	Disable.
dnd	The extension you are trying to reach has do-not-disturb activated. Please hang up.
dot_tip	Dot.
enable	Enable.
gateway	Gateway.
group busy	Please hold. All lines are busy.
hang-up	Your call is being disconnected. Thank you for calling.
hangup2	This call will be disconnected in one minute.
ip_tip	IP address.
IVR1	For call forward, press one. For voicemail, press two. Do not disturb: three. Call forking: four. Call waiting: five. Color ringback tone: six. For other extensions, press seven. To repeat this message, press nine.
IVR2	Enter the extension number, followed by the PIN then pound.
IVR3	Sorry, the feature cannot be activated.
IVR4	To obtain the current settings, press star; To return to the previous menu, press pound.
IVR5	The feature is now activated.
IVR6	Sorry, the feature cannot be activated.
wrong	Sorry, the feature cannot be activated.
IVR7	The feature is now deactivated.
IVR8	This is an invalid PIN, please enter a new PIN.
reenter	This is an invalid PIN, please enter a new PIN.
IVR9	The current setting is___
setting	The current setting is___
IVR10	To activate do not disturb, press one. To deactivate, press zero.
IVR11	To disable voicemail, press zero. To forward all calls to voicemail, press one. To forward busy or no-answer calls to voicemail, press two.
IVR12	To listen to the color ringback tone, press star. To change, press two, To disable, press zero. To return to the previous menu, press pound.
IVR14	To set the target number, press one.
IVR14A	To disable call forking, press zero. To enable and set destination number, press one.
IVR15	Enter the extension number, followed by the PIN. When done, press pound.

 Copyright © Redstone Systems, Inc

filename	element
IVR16	To disable call forward, press zero. To set the target number, press nine. To forward all calls, press one. To enable call forward busy or no answer, press two. To obtain the current settings, press star; To return to the previous menu, press pound.
IVR18	This is an invalid PIN, please enter a new PIN.
netmask	Netmask.
noanswer	There is no answer. Please enter another number, or hang up.
nocircuit	All circuits are busy. Please try your call again later.
nonumber	The number you have entered is not valid. Please check the number and enter again, or press zero for an operator.
offhour	Thank you for calling. We are currently closed. If you know your party's extension, enter it now.
operator	Please hold while your call is transferred to an operator.
operbusy	All operators are busy. Please enter another number or press star to hold.
port	Port.
record	Please record your message at the tone, and hang up when done.
tryagain	Your call cannot be completed, please try again later
version	Firmware version.
vm_all	Your call will be forwarded to voicemail. Leave your message at the tone and hang up when done.
vm_busy	That line is busy. Leave your message at the tone and hang up when done.
vm_fail	Your call cannot be completed, Leave your message at the tone and hang up when done.
vm_noans	Your party did not answer. Leave your message at the tone and hang up when done.
webport	Web access port
welcome	Thank you for calling. If you know your party's extension, enter it now, or press zero for an operator.
vm_new	___ new voicemail messages.
vm_no	You have no voicemail messages.
vm_old	___ saved voicemail messages.
vm_pre	You have ___
vm_prompt	To repeat the message, press one. To delete, press two. To listen to the next message, press three.
wakeup	Hello, this is your scheduled notification.
btime	Sorry, you are not authorized to make calls at this time, please contact the administrator.
binternal	Sorry, you are not authorized to make outgoing call, please contact the administrator.
lock	Sorry, your extension is locked. Please unlock it.
bres	Sorry, you are not allowed to call this number.

 Copyright © Redstone Systems, Inc

filename	element
bdomestic	Sorry, you are not authorized to make international calls, please contact the administrator.
blocal	Sorry, you are not authorized to make long distance calls, please contact the administrator.

2.9.22 Dual hot standby (REX1000)

The two REX1000 can be deployed as dual hot standby, so that when the master device is abnormal, the slave device will be automatically enabled to ensure uninterrupted calls.

Follow the steps below to configure dual hot standby.

Step 1 Depending on the site network, plan the following three IP addresses before configuration

- Master device IP address: fixed IP address.
- Slave device IP address: fixed IP address, must be in the same network segment as the master device.
- Virtual IP: Fixed IP address. is the IP address presented externally by the master and slave devices and must be in the same network segment as the master and slave devices.

Step 2 Configuring the master device

1. The functional configuration of the device for network, extensions, outside lines, etc. is omitted.
2. Enter the Dual Machine Hot Standby interface, checkEnableand set itas the master device.
3. Configure the IP address of the paired device (i.e., slave device), enter and record the authentication key, which you can define by yourself, as long as the master and the slave devices are identical.
4. Enter the virtual IP address and mask information.
5. Fill in the gateway address of the device as the network detection node. The

 Copyright © Redstone Systems, Inc

device sends a ping request to that address to test network connectivity. If no response is detected, it indicates that the current device is in an operational error state.

6. Configure the healthy heartbeat interval and monitor heartbeat timeout.

Step 3 Configuring Slave Devices

1. Go to the Dual Hot Standby interface, check Enable, and set it as aslave device. Configure the IP address of the paired device (i.e., the master), enter the same authentication key as the master, and other configurations, then the other configurations of the slave device are automatically synchronized on the master.

Figure 2-90 Dual Machine Hot Standby Interface

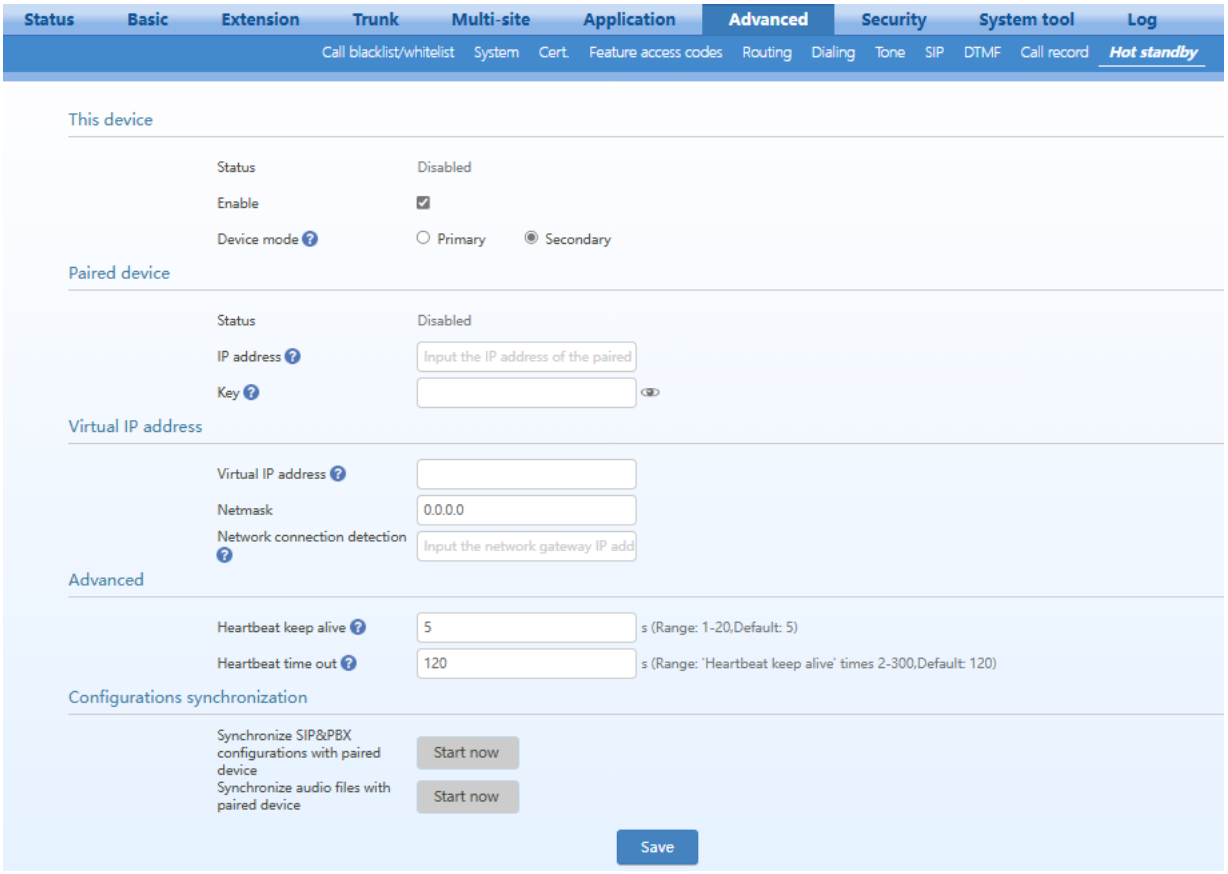


Table 2-49 Parameter description of the master-standby switchover

Item	Definition
This equipment	
Status	Displays the current device operating status: ● Not Enabled: The current device does not have the dual machine hot standby feature enabled ● Active: current device is working ● Standby: the current device is in standby mode ● Operation error: the current device failure status, usually the network is not available ● Waiting: Waiting for paired devices to come online
Activate now/Activate the paired device	Used to manually switch between master and standby states, generally used for maintenance management, such as firmware upgrades. ● Activate Pair: When the device is active, click this button to enable the paired device, this device is in standby mode. ● Set to Active: When the device is in standby mode, click this button to put this device into active mode and pair the device as standby.
Enable	Used to enable or disable the dual machine hot standby function.
Device mode	Select the current device as the master or slave. Dual hot standby requires two devices to be used in pairs, one as the "master" and the other must be configured as the "slave". When both devices are started at the same time, the master device will enter the "active" state and the slave device will enter the "standby" state.
Paired device	
IP address	The IP address of the paired device, if the current device is the master, then enter the address of the slave.
Key	Used for transmission encryption to ensure security, the authentication keys of the master and slave devices must be the same. It is recommended to enter 8 digits of letters or numbers.
Virtual IP address	
Virtual IP address	The IP addresses presented externally by the two devices in the dual hot standby group. The same network segment as the master and slave device addresses.
Subnet mask	The subnet mask of the virtual IP address.
Network monitoring node	Used to detect whether the current network environment is normal, it is recommended to fill in the gateway address of the device. The device sends a ping request to that address to test network connectivity. If the detection fails, the device is in an operational error state. Need to make sure that this IP address does not disable pinging.
Advanced settings	
Heartbeat keep alive	The device in the active state sends heartbeat packets to the device in the standby state at this interval. Default 10 seconds.
Heartbeat timeout	If the standby device does not receive a heartbeat packet from the active device within this time, it will automatically switch to the "active" state and take over all services.

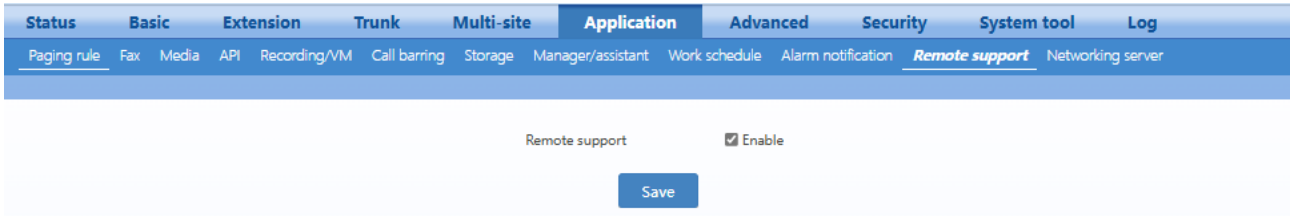
Step 4 Save the settings.

 Copyright © Redstone Systems, Inc

2.9.23 Remote Support

Users can enable remote support from the Application Services > Remote Support page.

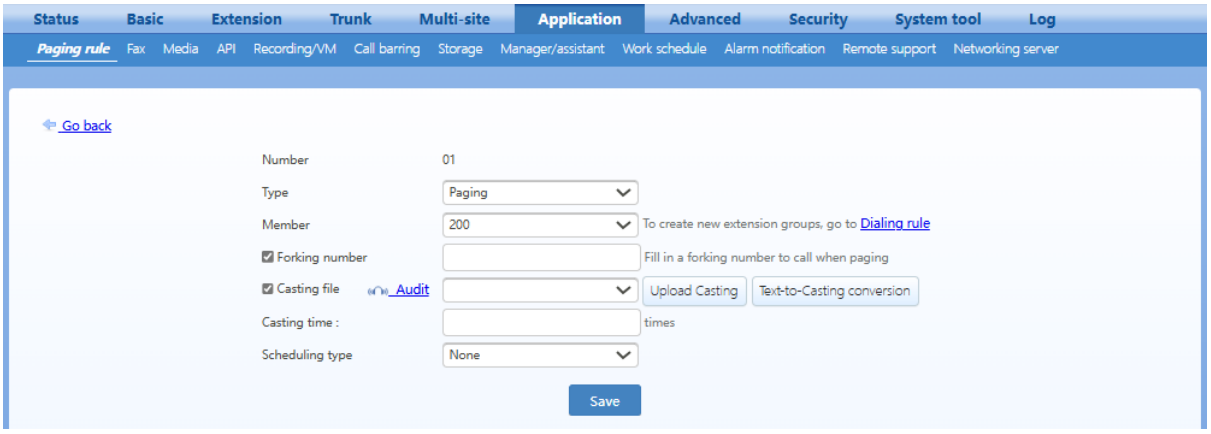
Figure 2-91 Remote Support Interface



2.9.24 Paging Rules

Users can click "Add" button in the Application Service > Paging Rulespage to set Paging rules in the pop-up page (support broadcasting to analog extensions, but do not support two-way broadcasting for the time being).

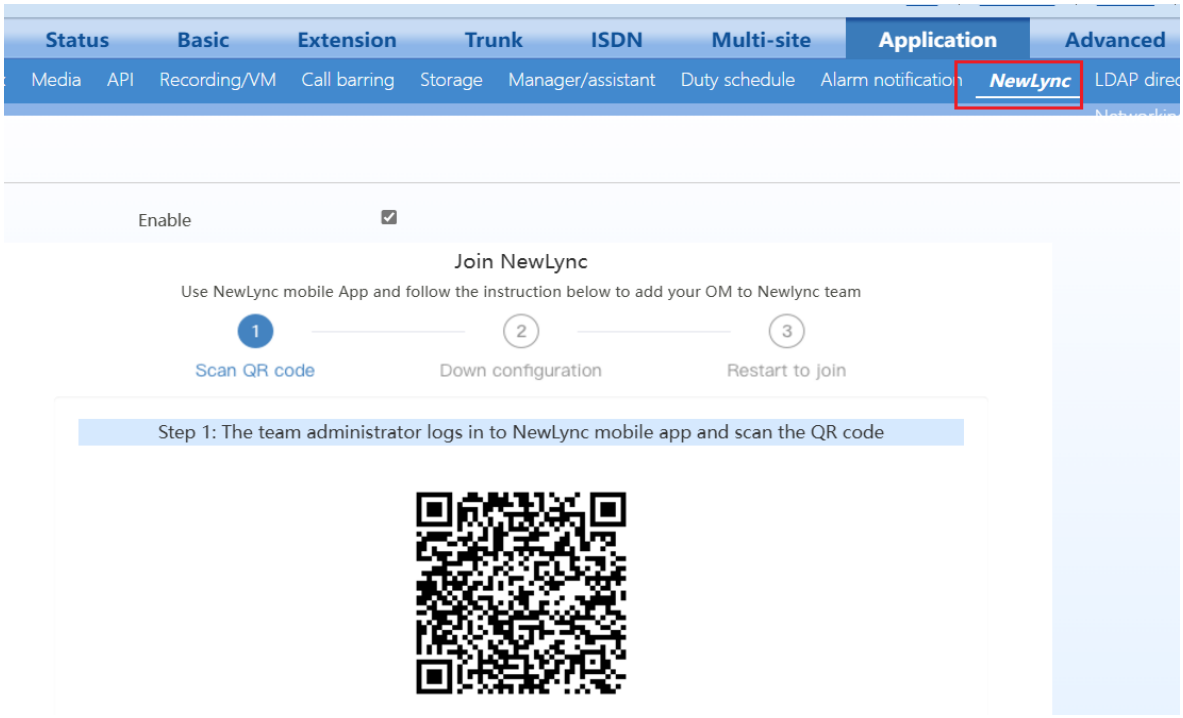
Figure 2-92 Broadcast Rule Setting Screen



2.9.25 NewLync Service

Users go to Application Services>Cloud Collaboration Service, check "Enable" to enable the functions of NewLync App, PC and desktop phones on the same vibration, call relay and so on.

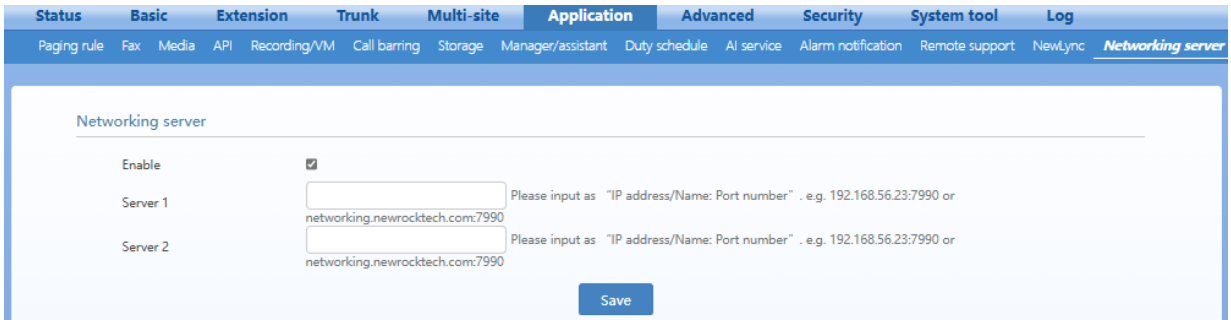
Figure 2-93 NewLync Service Settings screen



2.9.26 Networking Server

Users go to Application Services > Network Server, check "Enable", and set the IP address (or domain name) and port of the network server. Grouping server addresses must not be duplicated or conflicts will occur.

Figure 2-94 Networking Server Settings Screen



2.9.27 Alarm Notification

The Alarm Notification feature allows users to set up automatic notifications to be sent to a specified phone number when a specific alarm occurs on the device.

Figure 2-95 Alarm Notification Interface

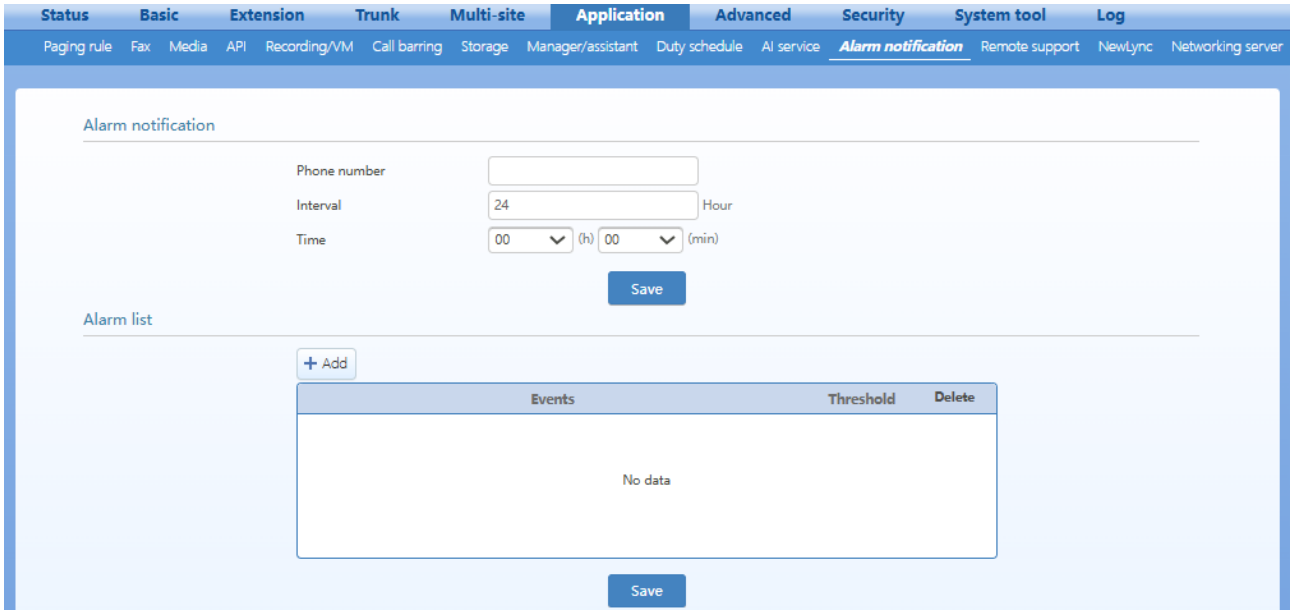
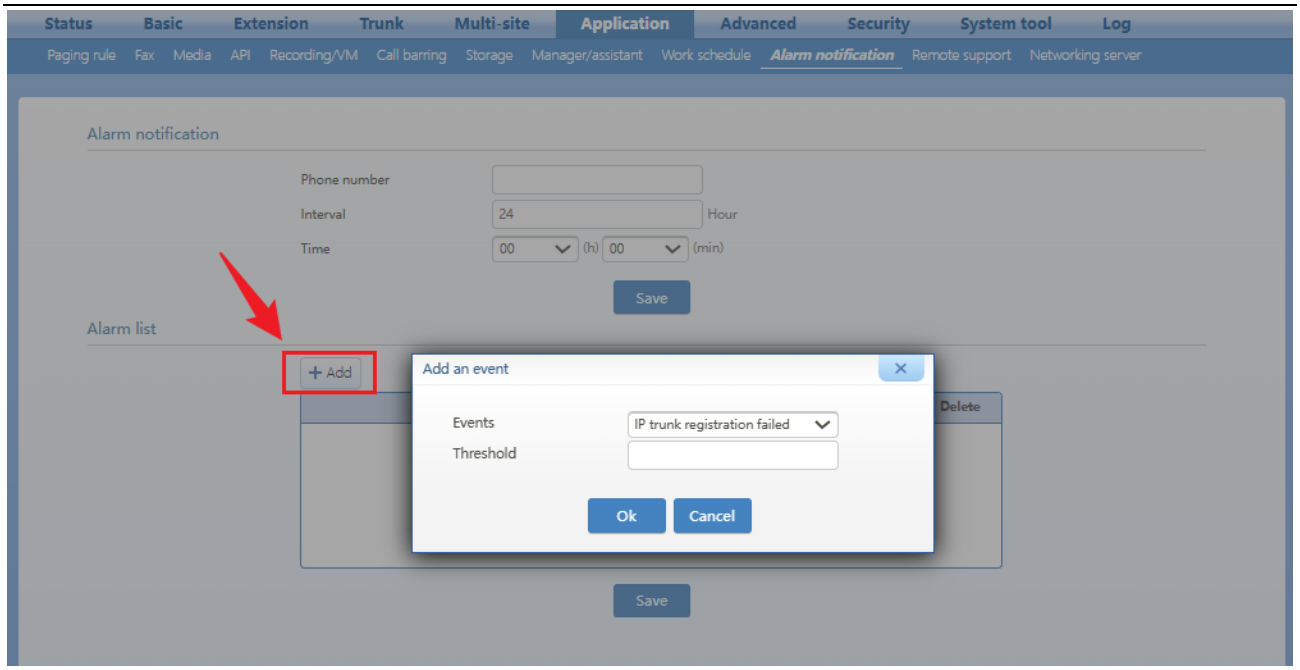


Table 2-50 Alarm Notification Parameter Description

	Definition
Alarm Notification Number	Setting up phone numbers to receive notifications
Alarm notification cycle	Specify how many hours to send alert notifications.
Alarm notification time	Define a specific point in time (e.g. XX time XX minutes) to trigger an alert notification

Step 1 Click + Add Alarm List

 Copyright © Redstone Systems, Inc



Step 2 Select alarm events and configure alarm thresholds

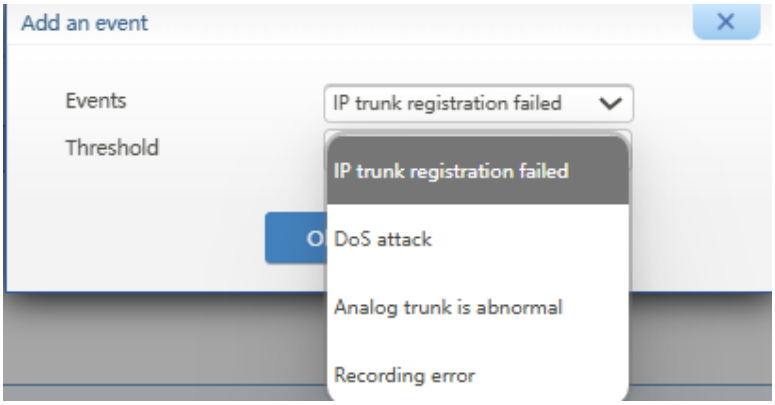


Table 2-51 Description of alarm notification options

	Definition
IP Relay Registration Failure	Refers to the failure of the device's IP trunk (usually a SIP outside line) to successfully register with an IP telephony service provider or external SIP server. Often this situation results in the inability to originate an external call over that outside line.
DoS attack	A DoS (Denial of Service) attack is a form of network attack in which an attacker exhausts the resources of a target system by sending it a large number of requests, thus preventing the service from responding to normal user requests.
Analog Outside Line Anomaly	Refers to a problem with the device's analog outside line (usually the FXS port) that prevents the outside line from being accessed properly to make outside calls or receive outside incoming calls.
Recording anomaly alarm	Problems with the device during the recording process may cause the recording function to not work properly. This may affect call recording, message recording, etc.

Step 3 Save Settings

 Copyright © Redstone Systems, Inc

2.10 Security Management

2.10.1Firewall

Users go to Security > Firewall to set upaccess white listing and static defenses.

2.10.1.1 Access white listing

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

With white listing enabled, only whitelisted IP addresses are allowed to access REX's Web or SSH services. In addition to the user-defined whitelist, the REX also provides the factory-built white list address 192.168.2.100.

The configuration steps are as follows:

Step 1 Go to Security>Firewall>Access Whitelist, click Add, and fill in the whitelist information. Up to 20 addresses can be added.

Table 2-52 Description of whitelisting parameters

Item	Definition
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, choosing from SSH, HTTP, HTTPS, and so on.
Delete	Delete the current whitelist information.

Step 2 Save the settings.

Step 3 Turn on white listing.



- To access the device via SSH, you also need to enable the SSH service of the device in theSecurity>Security Configurationpage.
- If you forget the set whitelist address and cannot access the device, refer to3.9 Forgetting to customize whitelist results in not being able to log in to the devicefor restoration.

 Copyright © Redstone Systems, Inc

2.10.1.2 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 > Firewall > Static Defense to open this configuration screen.

Figure 2-96 Static Defense Configuration Interface

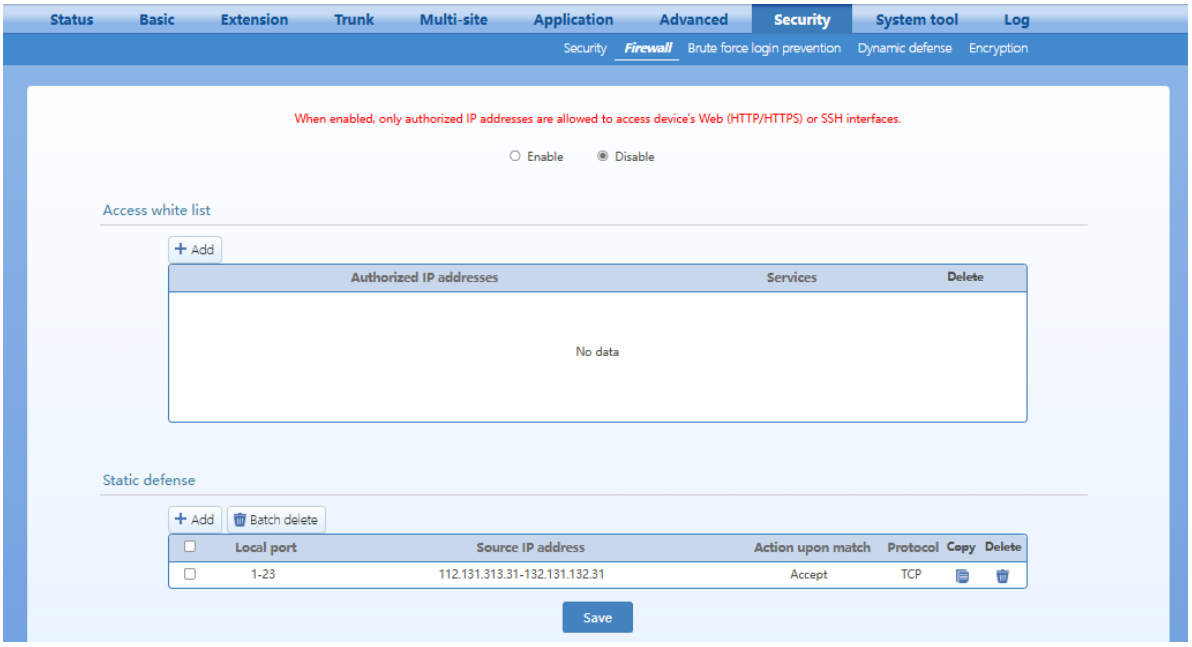


Table 2-53 Static defense parameters

Item	Definition
Enable/Disable	Configure whether to allow receiving packets from the source IP address when the rule matches.
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.
Protocol	Configure the protocol type, options include TCP, UDP, ICMP or any.

 Copyright © Redstone Systems, Inc

The following operations can be performed:

●New: Add a new rule;

●Copy :Copies the currently selected rule to the next one, making it easy to quickly add similar rules;

●Delete :Delete the current rule;

●Batch Delete: Delete the selected rules in batch.

Note

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

Typical example

The meaning of the example rule in Figure 2-88 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 192.168.120.60.

● Rule 3: Always prohibit ports 5060 and 5061 of the device from receiving packets from the source IP address 192.168.120.70 (regardless of protocol type).

2.10.2 Anti-brute-force account break-in

The main manifestation of a brute-force account is multiple logins 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 logins attempts and access whitelisting for Web logins to eliminate brute-force cracking at the source.

Login Retry Lockout Configuration

Once you have logged in, click Security > Brute Force prevention to open the configuration screen.

 Copyright © Redstone Systems, Inc

Figure 2-97 Anti-Violence Breach Account (Login Retry Lockout) Configuration Screen

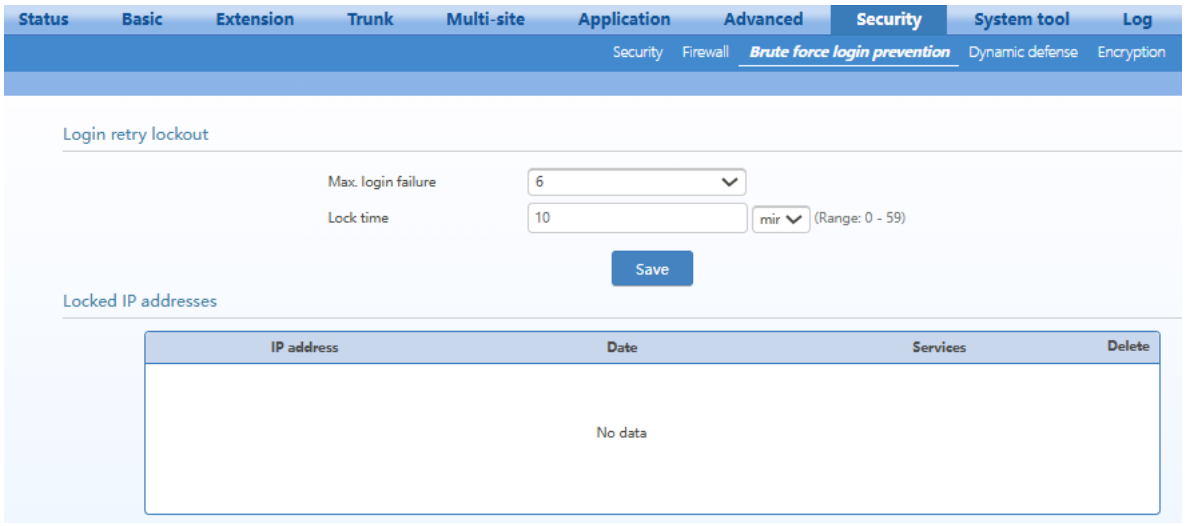


Table 2-54 Anti-brute-force account break-in (login retry lockout) parameters

Item	Definition
Max. login failure	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 time	Configure the lockout time for the IP address. After the lockout time is exceeded, the IP address will be unlocked, allowing access to the device again. The default is 10 minutes.

Locked list

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

Once you have logged in, click Security > Brute Force prevention to open the configuration screen.

Figure 2-98 Anti-Violence Breach prevention (Lock List) Screen

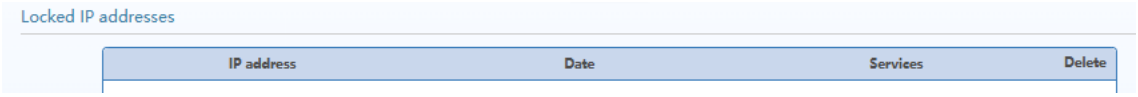


Table 2-55 Anti-brute-force account (lockout list) display information

Item	Definition
IP address	Locked IP address
Date	Lock the time of this IP address
Services	How this IP address accesses the device (Web or SSH)

 Copyright © Redstone Systems, Inc

The following operations can be performed:

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

2.10.3 Dynamic Defense

Dynamic blacklisting based on traffic rate limiting is a proactive defense mechanism of the device against unknown attack sources, which provides overload protection for the device by suppressing the packet rate and effectively resisting potential DoS/DDoS attacks.

Configure multiple dynamic defense rules so that when the packet rate received by the device exceeds the preset threshold in the rules, the received packets will be discarded, and at the same time, the IP address of the source of the attack will be added to the blacklist, and no more packets will be received from that address.

Rule Configuration

After logging in, click "Security > Dynamic Defense" to open the configuration interface.

Figure 2-99 Dynamic Defense Configuration Interface

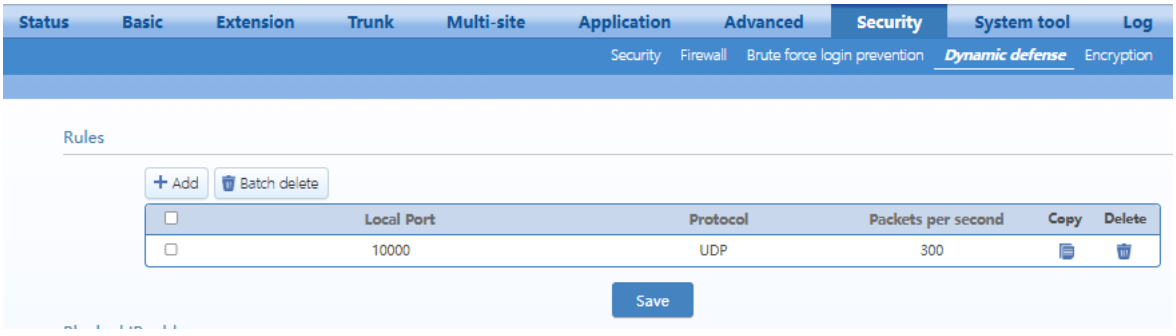


Table 2-56 Dynamic Defense (Rule Configuration) Parameters

Item	Definition
Local port	Configure the local port range on which the device receives packets. The configurable port range is 0 to 65535.
Protocol	Configure the protocol type, options include TCP, UDP, or any.
Packet per second	Configure the maximum packet rate that the local port is allowed to receive. When this value is exceeded, the IP address of the attack source is added to the defense list.

The following operations can be performed:

- Added: Add a new dynamic defense rule;
- Copy :Copies the currently selected rule to the next one, making it easy to quickly add similar rules;
- Delete :Deletes the selected rule;
- Batch Delete: Delete the selected rules in batch.

Defense List

Figure 2-100 This defense list is deleted after the device reboots. Dynamic Defense (Defense List) Interface

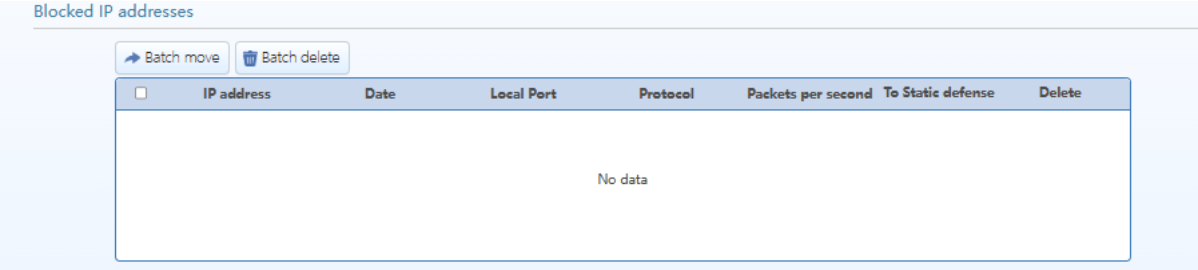


Table 2-57 Dynamic Defense (Defense List) Display Information

Item	Definition
IP address	The IP address of the source of the attack detected by the device.
Date	The time at which the device detects the source of the attack and begins to defend against it.
Local Port	The port on which the attack source packet was received.
Protocol	Displays the protocol type.
Packets per second	Displays the packet receive rate threshold.

 Copyright © Redstone Systems, Inc

The following operations can be performed:

- Bulk Move: Move selected entries to static defense rules in bulk with three subsequent options:

Table 2-58 (Subsequent selection of (batch) mobile defense lists to static defense lists

Treatment	Definition	Applicable Scenarios
Block	Generated as a new "forbidden" rule in the static defense rules.	These entries have been identified as the source of the attack
Accept	Generated as a new "allow" rule in the static defense rules.	The entries have been identified as legitimate sources (especially for high volume scenarios such as call centers)
Cancel	Keeps the entry in the dynamic defense list and does not move it to the static defense list.	/

- Batch Delete: Delete the selected entries in a batch.

Typical example

The meaning of the example rule in Figure 2-88 is:

- Rule 1: No more than 20 UDP packets per second should be received on port 5060.
- Rule 2: No more than 50 TCP packets per second should be received on port 5060.

2.10.4 Call restriction

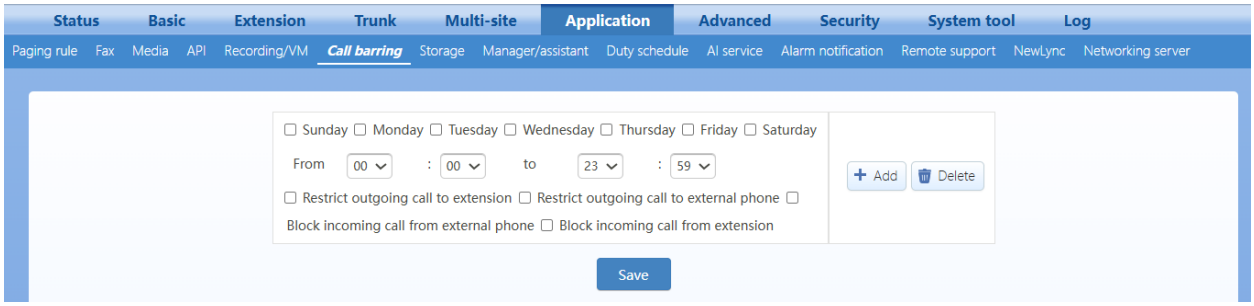
The device can restrict the outbound and inbound functions of an extension by time periods according to preset time and function templates.

The configuration steps are as follows:

Step 1 Go to Application Services>Call Restriction to set the time for the restriction to take effect and the inbound/outbound restrictions for extensions and outside lines. For example, on Mondays, no outside calls are allowed from 00:00 to 08:00. Click Add to add call restrictions.

 Copyright © Redstone Systems, Inc

Figure 2-101Call Barring Configuration Screen



Step 2 Save the settings.

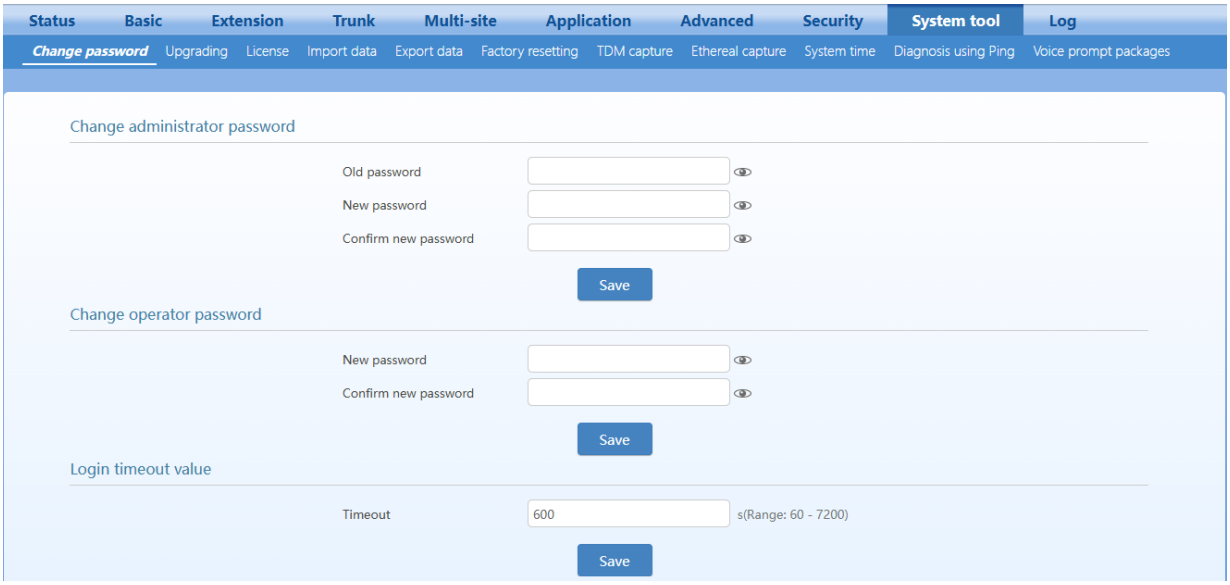
Step 3 Go to Extension Settings>Analog Extension/IP Extension>Settings and check the call restriction feature for the extension.

Step 4 Save the settings.

2.10.5 Change Password

Go to System Tools>Change Password to change the administrator password, operator password, and set the login timeout. Only the administrator has permission to change the password.

Figure 2-102 Change Password Interface

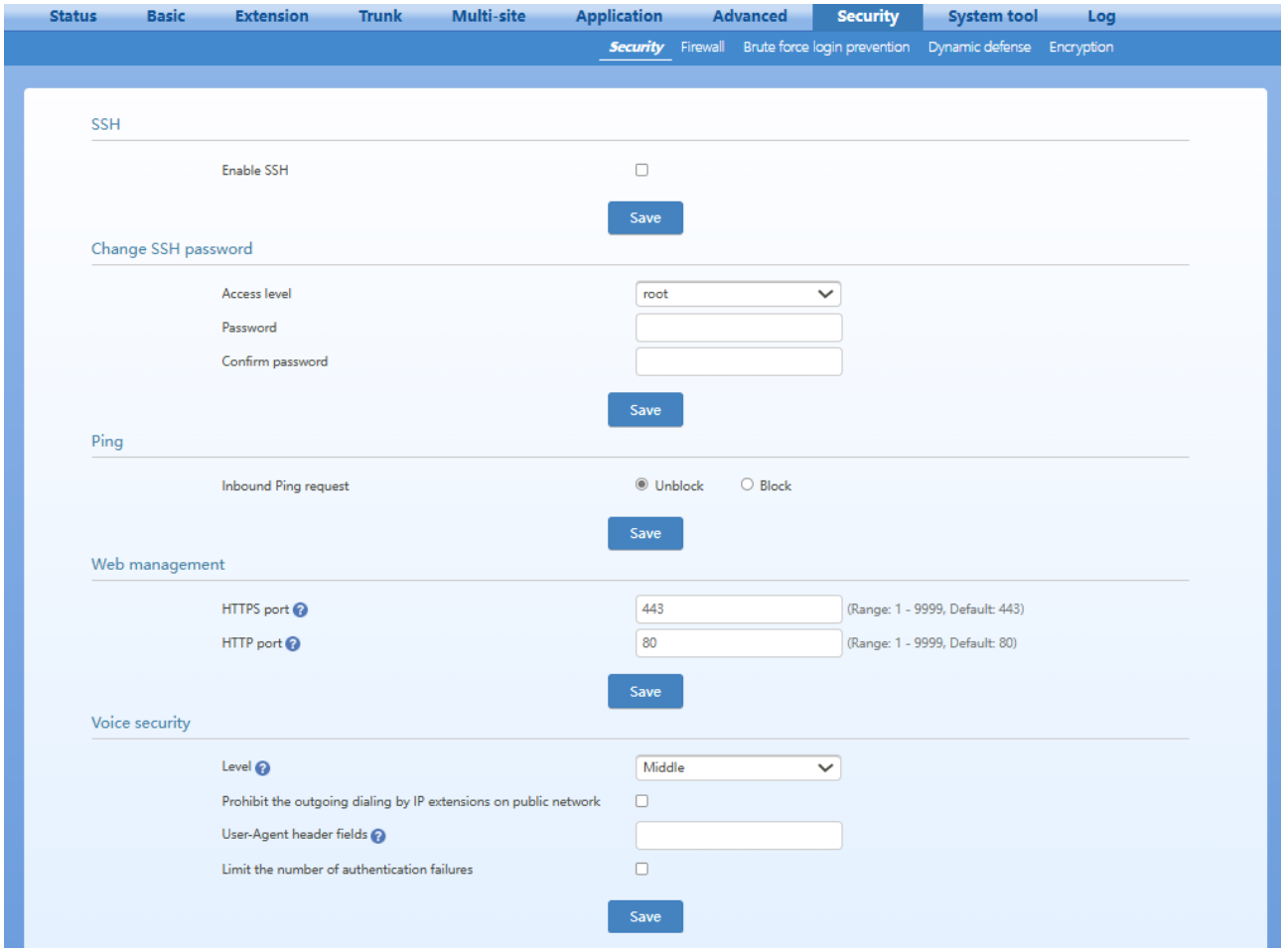


2.10.6 SSH

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

Go to Security>Security Configuration and turn on SSH.

Figure 2-103 SSH Configuration Interface



Item	Definition
Enable 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. This switch needs to be turned off promptly after use.
Access level	Both operator and root access rights.

 Copyright © Redstone Systems, Inc

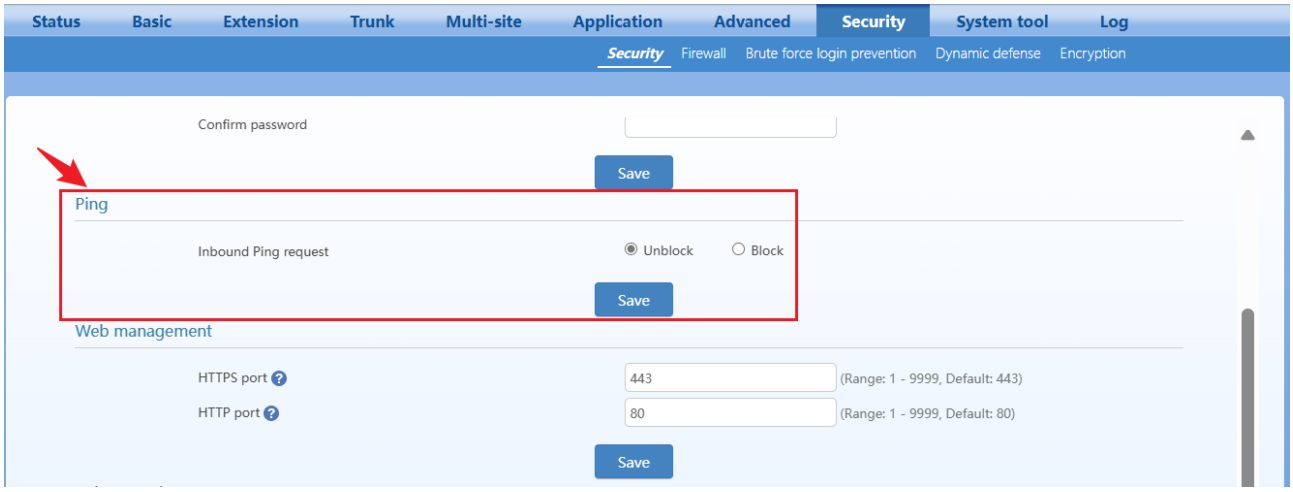
Item	Definition
Change Telnet/SSH password	Change the root user/operator user password for SSH access. The password needs to meet the following requirements: ● Length 6~20 characters ● Use a combination of letters plus numbers or special symbols for passwords ● No &, = or " " signs can be entered.

2.10.7 Ping

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

Go to Security >Security Configuration and configure the Allow or Disallow Ping feature.

Figure 2-104 Ping Configuration Interface



2.10.8 Web Management

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

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

Figure 2-105 Web Management Configuration Interface

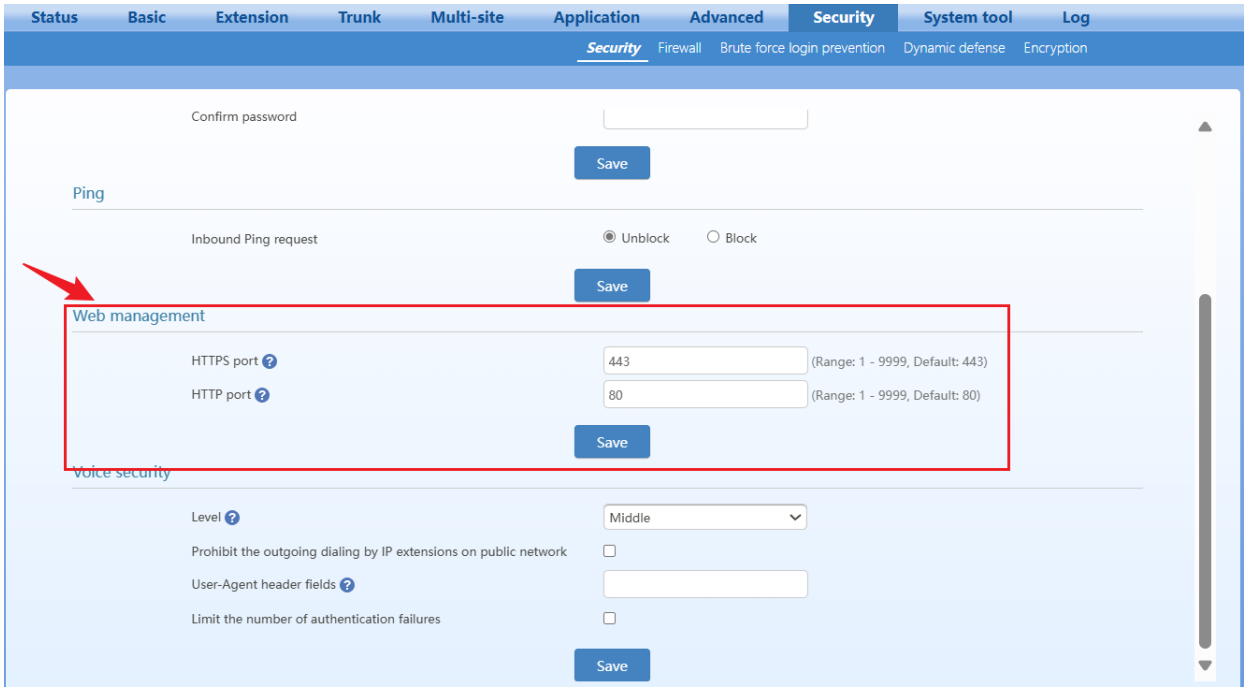


Table 2-59 Web Management Interface Parameter Description

Item	Definition
HTTPS port	Set the Web port when accessing the device using HTTPS protocol, the default value is 443.Value range: 1~9999The default value is 443, and the value range is 1~9999.
HTTP port	Set the Web port when accessing the device using HTTP protocol, the default value is 80, the value range: 1~9999.

 Copyright © Redstone Systems, Inc

2.10.9 Voice security

Go to Security>Security Configurationto configure voice security related features.

Figure 2-106 Voice Security Configuration Interface

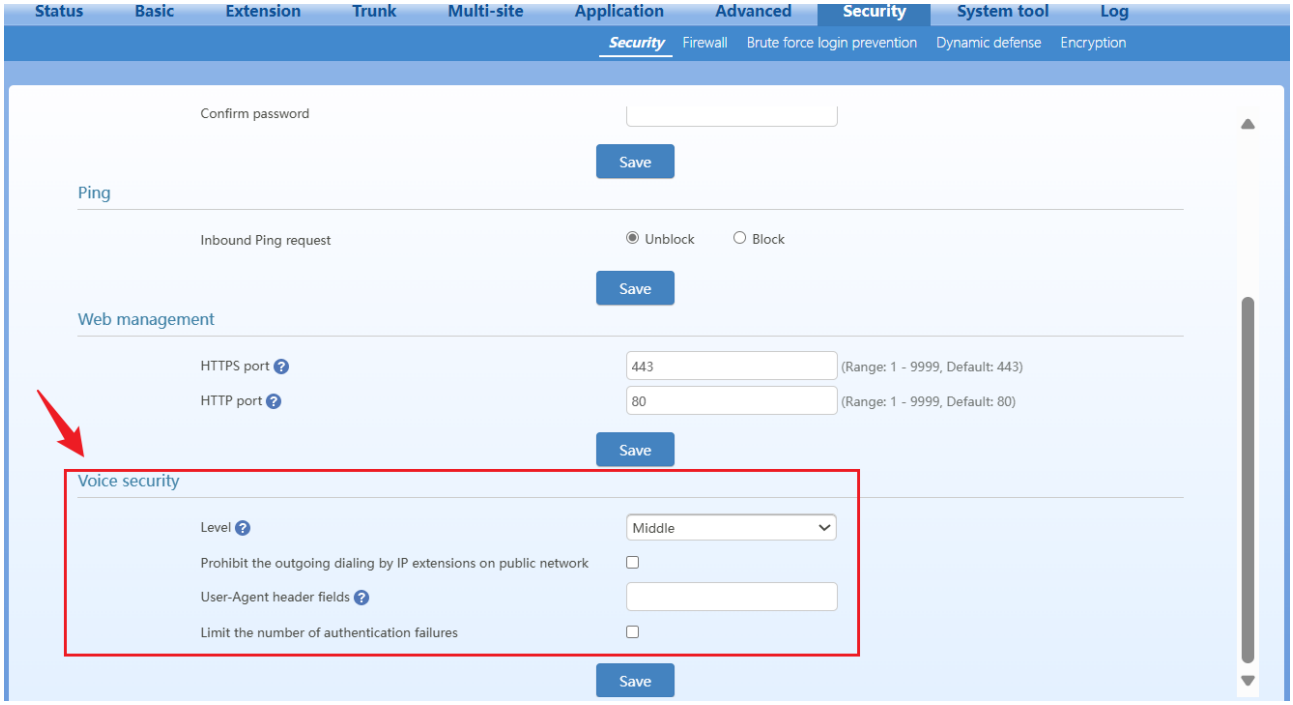


Table 2-60 Description of voice security interface parameters

Item	Definition
Level	The restrictions under each security level are listed below: • High security level: under the intranet, IP extensions with SIP signaling port greater than 10000 and the same registration password and number are not allowed to register; IP extensions in the extranet with the same registration password and number are not allowed to register; terminals in the extranet are not allowed to log in the Web management interface; • Security Level Medium: Same as the above restriction, but allows external network terminals to log in to the Web management interface; • Low security level: none of the above limitations.
Prohibit the outgoing dialing by IP extensions on public network	Outside IP extensions are only allowed to dial 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.

 Copyright © Redstone Systems, Inc

Item	Definition
Limit the number of authentication failures	When IP extension authentication fails more than the number of times specified in this parameter, the device will reject the registration of the IP extension. This IP extension is allowed to register only if the IP address of this extension is changed or the REX is restarted.

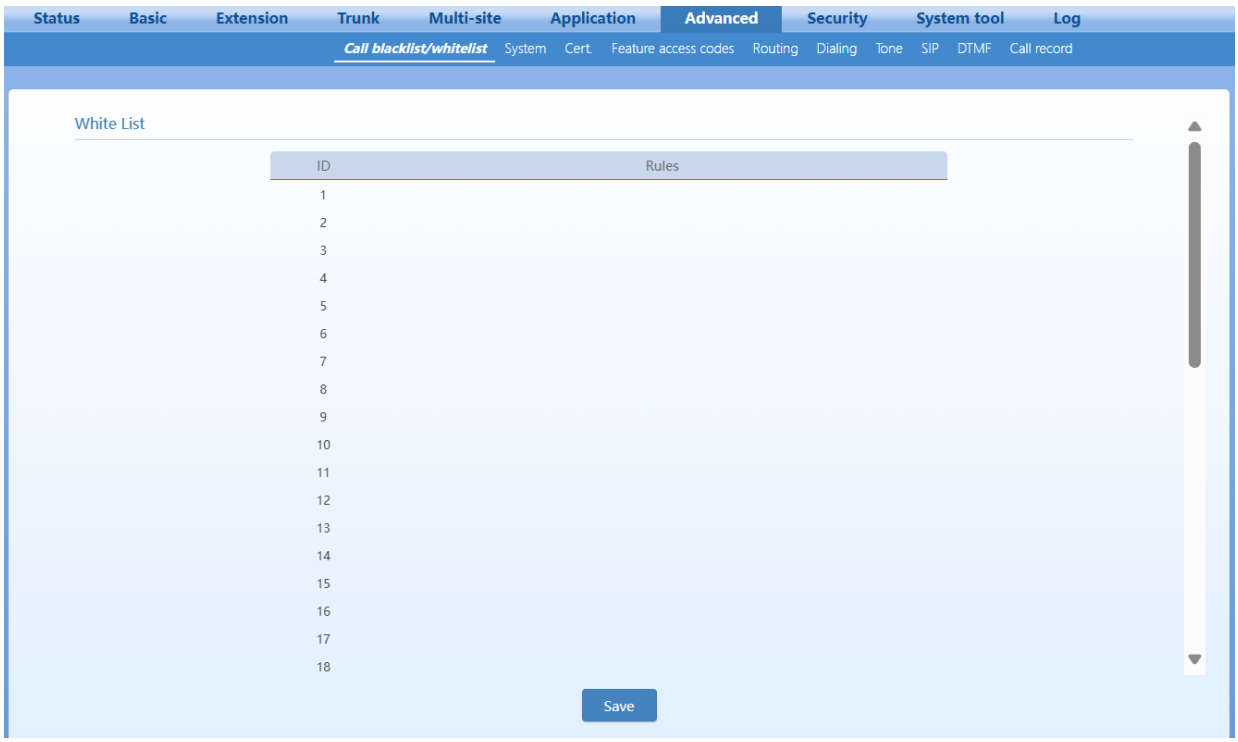
2.10.10 Black/White List

Users can set the analog/IP extension call black and white list in Advanced Settings > Call Black/White List.

Step 1 In a black/white list rule box, you can set one or more dialing rules (separated by commas).

Examples of black/white list rules: 2xxxx, 7xxxxxx, 86xxxxW2, 7. Where 2xxxx means 5-digit number starting with 2, 7xxxxxx means 7-digit number starting with 7, 86xxxxW2, W2 is the follow length limit (means 0 to 2-digit number can be followed), e.g.: 86xxxxW2 covers 86xxxx, 86xxxxx, and 86xxxxxx, and 7 means all numbers starting with 7.

Figure 2-107 Call Black/White List Configuration Screen

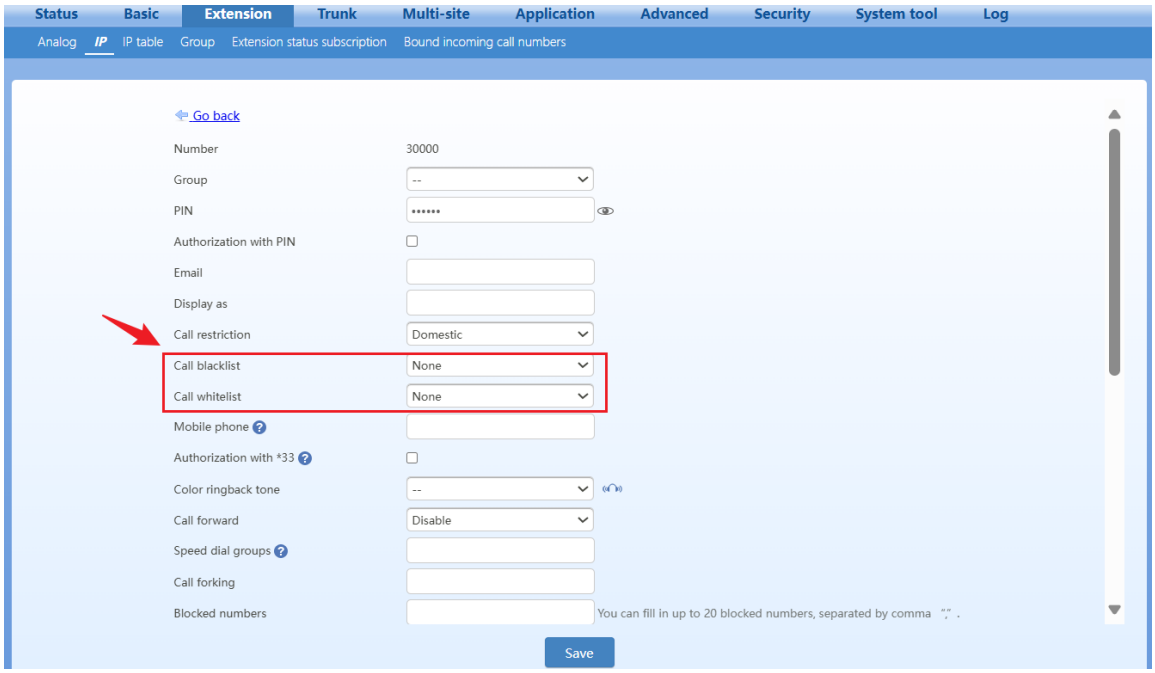


Note

1. Up to20 black/white list rules can be set at the same time.
2.When a user dials a number that does not meet the whitelist rules, the system announces a voice prompt "Your call privileges are insufficient, please contact the administrator". The rules in the Blacklist Rules box indicate that the user can dial other numbers except those that meet these rules. When the user dials a number that meets the blacklist rules, the system automatically broadcasts the voice prompt "Sorry, the system does not allow you to dial this number".

Step 2 Click Extension > IP, and click the "Settings" button at the end of the line of the IP extension that needs to set the black/white list rules (the analog extensions have the same settings as IP extensions) to enter the settings page, if you need to set the black list rules, click the drop-down menu on the right side of the "Calling Black List If you want to set black list rules, click the drop-down menu on the right side of "Call Black List" and select the black list rules you have just set (the rule in the No.1 rule box is "Customize 1", the rule in the No.2 rule box is "Customize 2", and so on), and the setup of whitelist rules is the same as this. The whitelist rules are set in the same way.

Figure 2-108 Extension Black/White List Configuration Interface



 Copyright © Redstone Systems, Inc

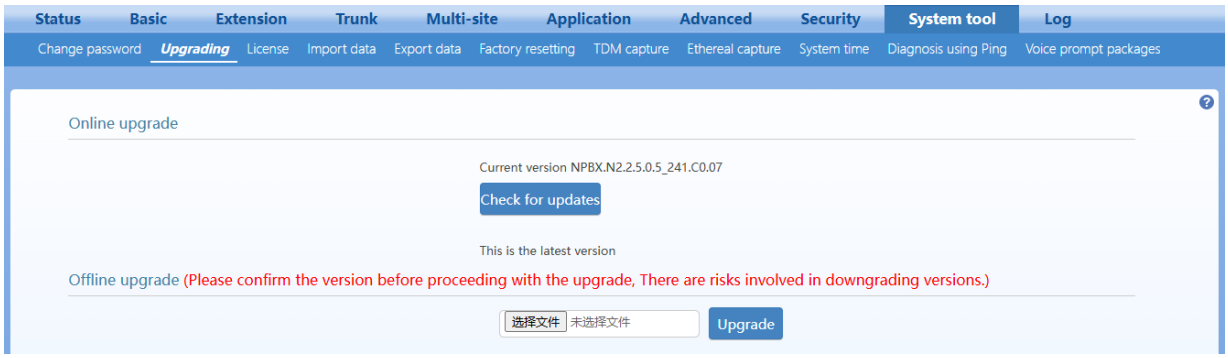
An extension can have both blacklist rules and white list rules, or just one of them.

2.11 System Maintenance

2.11.1 Upgrading

Go to System Tools > Upgrading, upload the upgrade package file and follow the prompts to perform the upgrade operation.

Figure 2-109 Software Upgrade Interface



Online Upgrade

Step 1 Go to System Tools>Software Upgrade to see if a new version is available.

Step 2 If the page shows that the latest version is available, you can click Upgrade Now and the device will automatically get the upgrade package from the Redstone server and upgrade. To learn about the new version, you can clickto view the version changelog.

Local upgrade (including kernel upgrade)

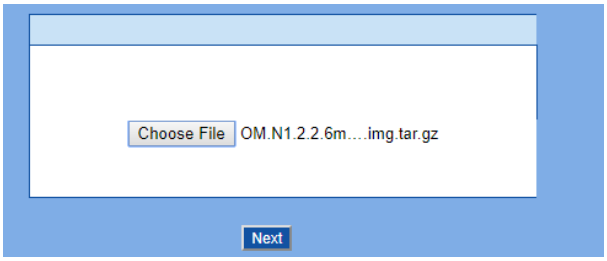
Step 3 Go to System Tools>Software Upgrade, upload and upgrade the "Intermediate Version File" xx.advanced_spe.tar.gz and follow the Definition.

Step 4 After the successful upgrade of "Intermediate Version", the browser automatically jumps to the second upgrade interface, select the "Final Version File" xx.img.tar.gz, and follow the Definition.

Note: If you are not automatically redirected to the secondary upgrade page, please enter your IP address and refresh it manually.

 Copyright © Redstone Systems, Inc

Figure 2-110 Secondary Upgrade Page



Note: To obtain the latest software update package, please contact the manufacturer

Local upgrade (no kernel upgrade)

The current configuration will not change after the upgrade. Before upgrading, please go to System Tools>Configuration Exportto export the current configuration as a backup.

Step 1 Go to System Tools>Software Upgrade, browse and upload the upgrade file (no need to unzip it, just upload it).

Step 2 Click Browseand select the tar.gz file stored in your local path.

Step 3 Click Upload to upload the upgrade file to the device.

Step 4 After successful upload, follow the prompts to upgrade.

Note

- Online upgrade takes about 15 minutes, other upgrades take about a few minutes, please do not upgrade 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.

2.11.2 Configuration Maintenance

Go to System Tools>Configuration Import/Configuration Export/Restore Factory Configuration/Functional Licenseto import/export the device's configuration file or restore the current device's configuration to the factory defaults, and upload the functional license file.

 Copyright © Redstone Systems, Inc

Figure 2-111 Configuration Import Screen

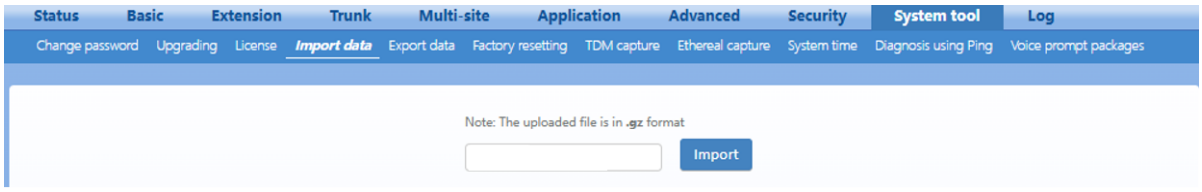


Figure 2-112 Configuration Export Screen

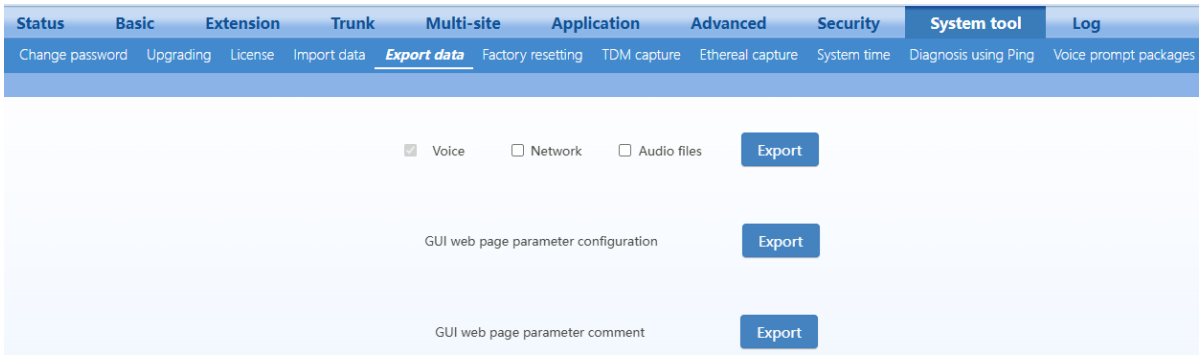
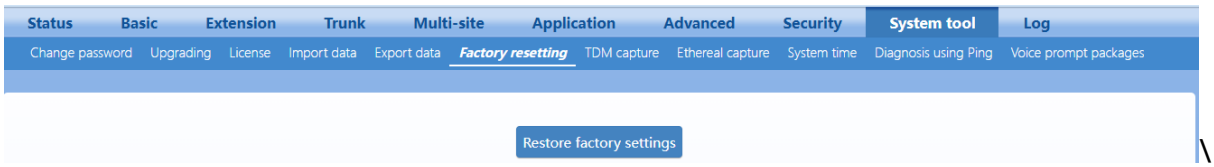


Figure 2-113 Restore Factory Configuration Interface



\

Figure 2-114 Functional License Configuration Screen



Note

- Do not power down, disconnect, or reboot the device during configuration import. After successful import, the device will reboot automatically.
- 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.

 Copyright © Redstone Systems, Inc

2.11.3 Reboot

Click Reboot at the top right of the interface to reboot the device through the web interface.

Figure 2-115 Reboot Screen

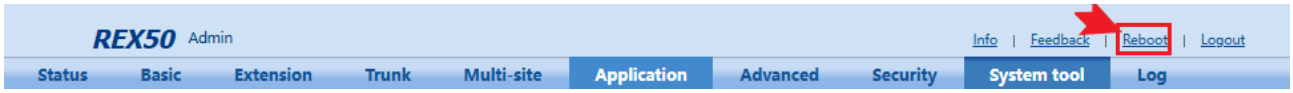


Table 2-61 Restarting the Configuration Interface

Item	Definition
Reopen	Overall reboot of the device hardware and software.

2.11.4 Port Signal Capture (Not supported by REX1000)

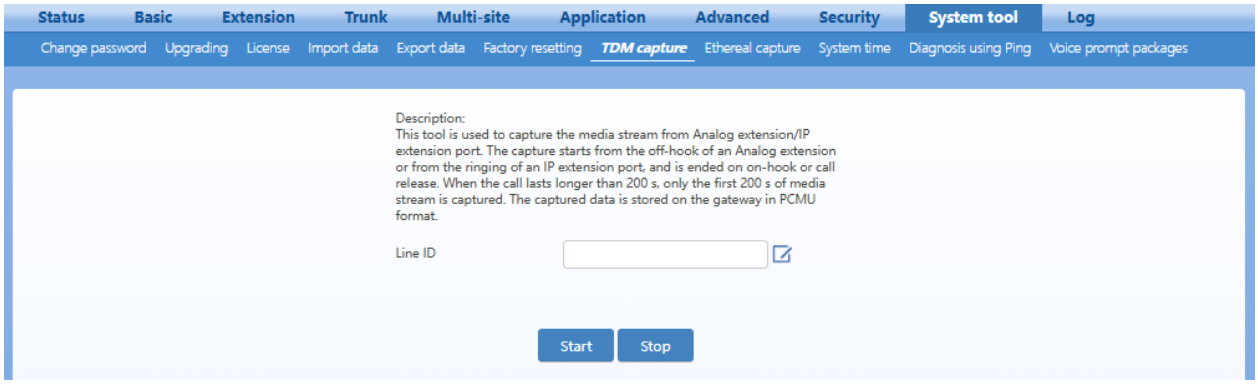
Port Signal Capture is to record the voice signals of analog ports, and the recorded voice signals can be used to analyze voice anomalies, such as caller ID anomalies, voice noise, and voice single pass. The device provides real-time port capture tool, the maximum allowable capture time is 200 seconds, more than 200 seconds capture automatically stops, the data is automatically discarded. The captured signal is temporarily stored in the device in PCMU encoding format, and the file is automatically downloaded when capturing stops.

Step 1 Go to System Tools>TDM capture and select the line port where you need to get the signal and click OK.

Port Capture begins when the call is established and terminates when the call ends.

 Copyright © Redstone Systems, Inc

Figure 2-116 Port Capture Interface



Step 2 Click Start toinitiate the capture.

Step 3 Create a test call for the line type (FXS port off-hook, or FXO port inbound) and end the call when you have completed the test content.

Step 4 Click Stop toend the capture. After the device prompts to download and pops up the Save Path prompt box, select the path where the packet is stored.

Recorded voice files can be opened for analysis using Cool Edit software. If you need help, you can send documentation and a description of the problem to globalmarketing@redstonesystems.com. If you need help, you can send the file and a description of the problem to, and a Timeless technician will analyze it and help you.

2.11.5 Ethereal capture

Ethereal 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. The maximum size of dump.cap is 2MB and the device can generate up to three packet files.

Step 1 Go to System Tools>Ethereal Capture and click Start Capturing Packets.

 Copyright © Redstone Systems, Inc

Figure 2-117 Data Capture Interface



Step 2 Perform problem reproduction operations, such as establishing a one-way call.

Step 3 Click Stop, the device will automatically prompt the download and pop up the save path prompt box, you can customize the path where the packet is stored according to your needs.

Step 4 Documents and problem descriptions can be sent to globalmarketing@redstonesystems.com.Our technicians will help you to analyze and solve the problem. For your own review, you can use Wireshark software to open the file.

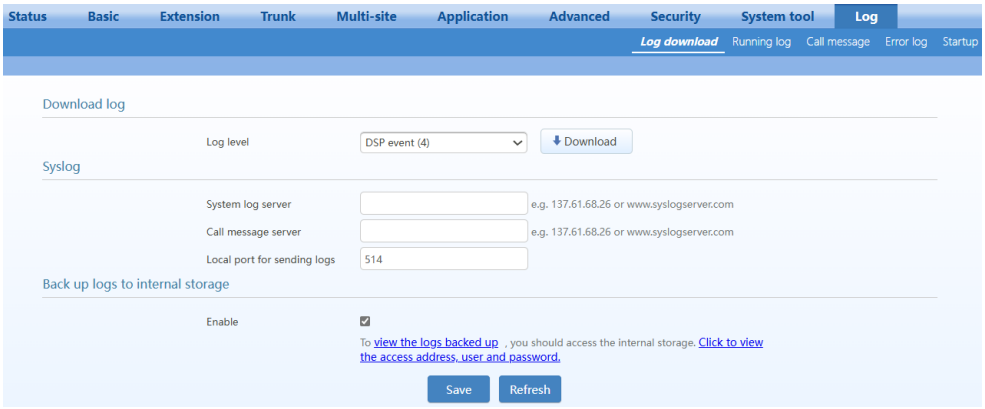
2.11.6 Log management

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

The logs of REX20/REX50 are stored in memory by default and have a default built-in storage capacity of 3GB for backing up the logs (the capacity can be modified from built-in storage inApplication Services > Storage Management); the logs of REX200/REX200-A/REX500 are stored in memory by default and can be backed up in the built-in storage; the logs of REX1000 logs are stored in memory only. Only the latest log information is retained in memory and will be cleared after a reboot. Logs in the built-in storage are not cleared by a reboot.

Logs in the built-in storage can be downloaded by simply following the interface prompts to the access path to the built-in storage.

Figure 2-118 Log Download Interface



 Copyright © Redstone Systems, Inc

In-memory logs can be downloaded from the interface. Here are the steps to download.

Step 1 Go to Logs>Log Download, select the log level and click Save.

Step 2 Perform problem reproduction operations, such as establishing a one-way call.

Step 3 Click download, the device will automatically prompt to download, and pop-up save path prompt box, you can customize the data packet storage path as needed.

Step 4 Documents and problem descriptions can be sent to globalmarketing@redstonesystems.com Our technicians will help you to analyze and solve the problem.

If you need to collect log information throughout the entire process, you can configure a log server. You need to select the logging level first, and then configure the logging server and port information.

Table 2-62 Log Download Interface Parameter Description

Item	Definition
Log level	The syslog defaults to level 4. Select the log level according to the actual problem. Note: Each time the device reboots, it will restore the syslog level to the default.
System log server	Fill in the log server (Syslog) IP address or domain address, if you need to fill in the port, separated by ":", such as 192.168.1.100:518. When this parameter is configured, the system stores the logs on the server and the device no longer generates system logs locally.
Call Message Server	Used for docking Syslog server, fill in the Syslog server IP address or domain name, if you need to fill in the port, you need to use ":" to separate, such as 192.168.1.100:518. When this parameter is configured, system call messages will be sent to the configured server and no call messages will be generated locally by the device.
Local port for sending logs	Local message sending port for interfacing with the Syslog server. The default is 514, which generally does not need to be changed.
Log backup	When enabled, logs are backed up in the built-in storage. The built-in stored logs can be kept for a long time and will not be lost after a device reboot. Not enabled by default.

2.11.7 Operational Information

Operational information is used to record the operational status of the device and also to monitor events occurring in the device.

Go to Log>Run Infoand click Refresh to view the current system run info.

Figure 2-119 Operation Information Screen

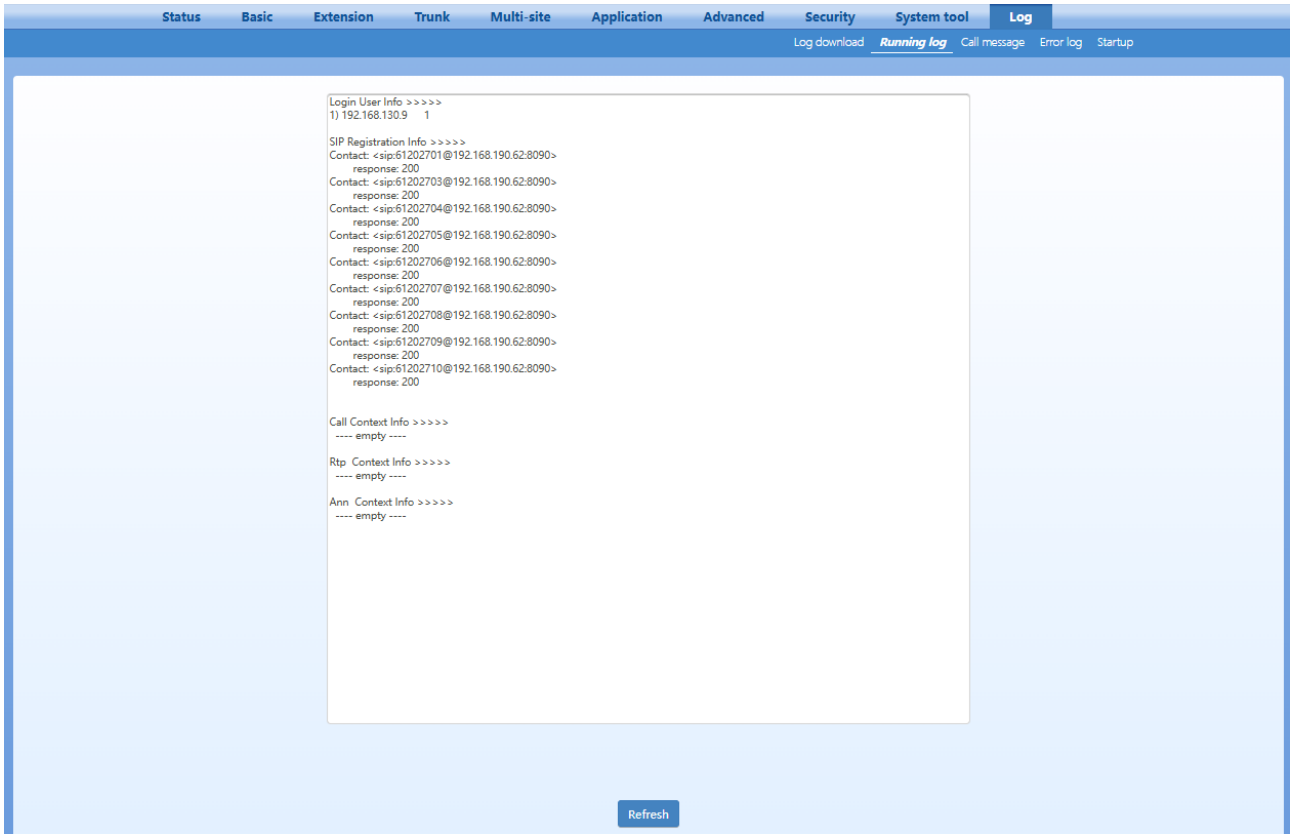


Table 2-63 Operational Information Interface Parameters

Item	Definition
Login User Info	Displays the IP address currently logged into the web interface and its privileges. where the number displayed after the IP address represents the privileges corresponding to that address: • 1: Administrator privileges. • 2: Operator privileges. • 3: User browsing mode.
SIP Registration Info	Displays the device's enrollment • Not enabled: The registration server address was not entered. • Latest response: the latest registration response message, 200 means the registration was successful. • No response: No response was received from the registration server. It may be caused by IP network failure or registration server unreachability, etc.
Call Context Info	Displays the current call status.
Rtp Context Info	Displays the voice channel used for the call.
Ann Context Info	Displays the IVR voice file resource.

 Copyright © Redstone Systems, Inc

2.11.8 Dual-System Switching Method

Effective October 21, 2025, the system switching mechanism has been optimized. The automatic system switching function triggered by eight consecutive power outages has been discontinued. System switching must now be initiated manually by the user through coordinated operation of the RESET button and STU indicator light. The procedure is as follows:

Step 1 Ensure the device is powered off. Press and hold the RESET button before powering on. After powering on, release the button within 3 seconds when the STU indicator flashes yellow rapidly (a mix of red and green flashes). If the button is not released within the specified time, the system will bypass the dual-system switching process.

Step 2 Under the STU indicator light, repeat the following steps three times:

When the STU light is solid red, press the RESET button;

When the STU light is solid green, release the RESET button.

Note Each press and release operation must be completed within 2 seconds; failure to do so will skip the system switching process.

Step 3 Verify the system switch result.

After completing the above operation three consecutive times, the STU light will begin to flash rapidly:

Green flash indicates switching from System B to System A;

Red flash indicates switching from System A to System B.

Note When performing a system switch operation, ensure a stable power supply to prevent power loss during the process.

 Copyright © Redstone Systems, Inc

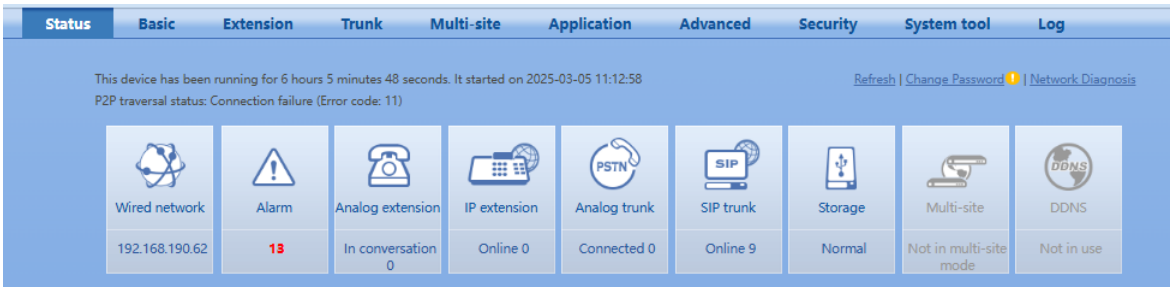
If multiple attempts fail to complete the switch, you may manually switch the system partition by entering the U-Boot command line.

2.12 Equipment Maintenance Information

2.12.1 Operational status

Enter the status to view the device's network parameters, alarms, extension and outside line status, storage usage status, grouping, dynamic domain name, and other information.

Figure 2-120 Running Status Interface



2.12.2 Alarms

After entering the status page, move the mouse over the alarm icon to view the alarm messages of the device.

According to the severity level from low to high, the alarm messages are categorized into security alerts, orange alarms, and red alarms.

 Copyright © Redstone Systems, Inc

Figure 2-121 Alarm Interface

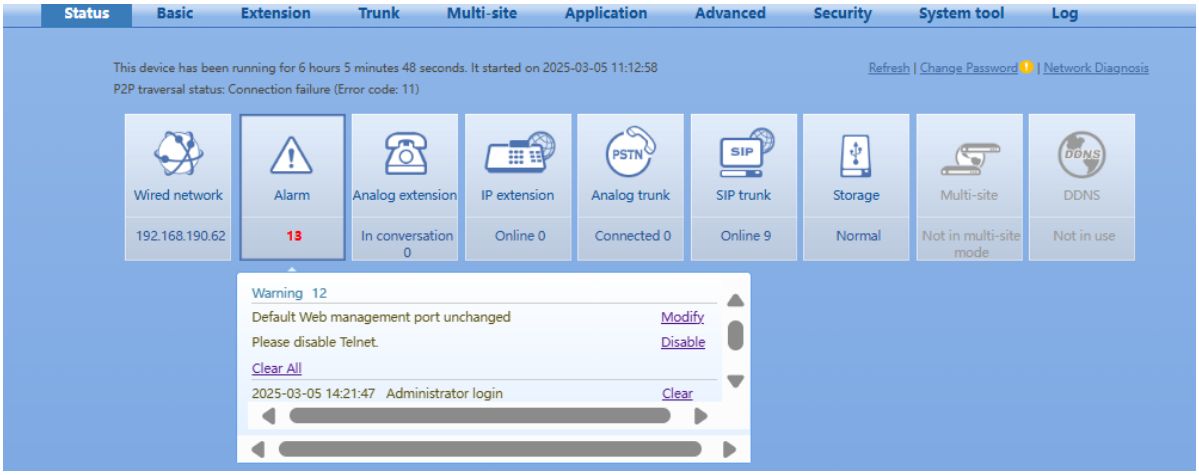


Table 2-64 Classification of alarm messages

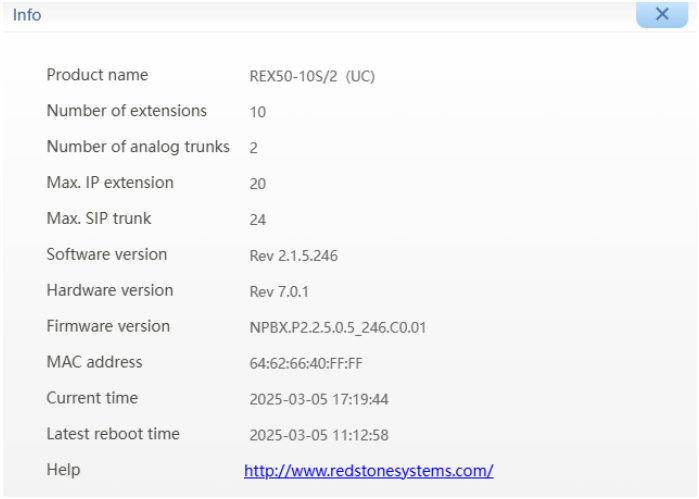
Item	Definition
Safety alerts	IP Outside Line Registration Successful
	Modify the SIP port
	WAN connected
	Operator Login
	Administrator Login
	IP address change
	FXO port wired
	FXO port not wired
Orange alerms	Change administrator password
	Wrong login password
	Change operator password
Red alerms	Device reboot
	software reboot
	IP outbound registration failure
	IP extension registration failure
	DNS resolution failure
	The network port connection has been disconnected
	be subjected to a SIP attack

2.12.3 Product Information

Click Product Informationat the top right of the interface to view the device model, version, number of extensions, MAC address and other information.

 Copyright © Redstone Systems, Inc

Figure 2-122 Product Information Screen

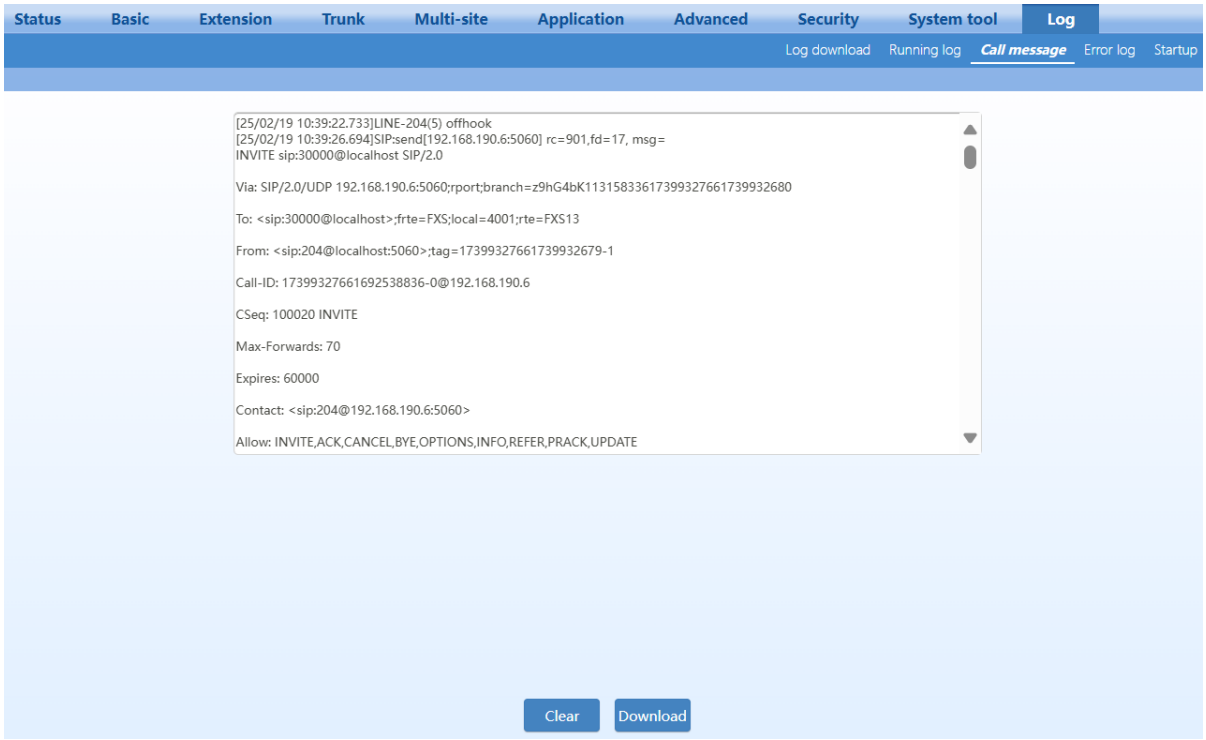


2.12.4 Call Messages

If there is a problem with a call, you can find the cause via the call message.

Step 1 Go to Log>Call Messages to clear the current call message.

Figure 2-123 Call Message Screen



Step 2 Perform problem reproduction operations, such as establishing a call all the way through.

Step 3 Click Download to save the call message file.

Step 4 Send documentation and a description of the problem to

globalmarketing@redstonesystems.com. A Swift Time technician will help you analyze and solve the problem.

2.13 Supporting Application Software

The following table shows the application software that accompanies the REX, in which the use of NeeHau Business Assistant, Hotel Management Docking Module, Zibo Billing Software need to open the device's API interface, for details, see 02.9.15 APIFor details, please refer to the following table. Softphones can be accessed as extensions by registering to the device through SIP, or they can be accessed through automatic secondary dialing to call each other through the devices outside line.

Table 2-65 List of applications

Item	Definition
Neehau Business Assistant	Provide extension users with practical functions such as incoming call pop-up, click dialing, call recording, note taking, customer information management, alarm clock event reminder and so on.
Hotel Management Docking Module	Cooperate with the hotel management system to realize the business of guest telephone records, wake-up call and telephone call authority control.
Zibo Billing Software	Provide bill statistics, bill setting, billing, real-time bill inquiry, report printing and other functions.

 Copyright © Redstone Systems, Inc

3 Common Problems

3.1 No number display for incoming calls

Phenomenon: When an analog outside call comes in, the phone displays the FXO port number instead of the caller's number.

Solution:

1. Check the wiring

   Connect the handset directly to the telephone line and check if the line is enabled for Caller ID. If the phone does not display the correct number, contact the operator. If the number is correct, observe whether the number is displayed before the first ring or after one or two rings.

2. Check device configurations

   Click Outside Line >Analog Outside Line to check if Caller ID is on and go toAdvancedto confirm that the Incoming Call Detection Mode (Pre-Ring or Post-Ring) matches the line.

 Copyright © Redstone Systems, Inc

3.2 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:

Click Logs>System Logs to view the IP Outbound Registration Status screen. The table below.

Table 3-1 Solution to SIP Outbound Registration Problems

Display content	Registration Status	cure
SIP Registration Info >>>>> Contact. <sip:61208000@192.168.250.5:5060> response. 200	Registration was successful.	Check the network configuration and wiring while analyzing the call SIP signaling.
SIP Registration Info >>>>> Contact. <sip:61208000@192.168.250.5:5060> No Response	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.
SIP Registration Info >>>>> Contact. <sip:61202000@192.168.250.5:5060> response. 404	Incorrect IP outbound registration number.	Contact your IP telephony service provider to confirm that the SIP outbound registration number is correct.
SIP Registration Info >>>>> Contact. <sip:61208000@192.168.250.5:5060> response. 403	Incorrect registration password.	Contact your IP telephony service provider to confirm that the SIP outbound registration password is correct.

 Copyright © Redstone Systems, Inc

3.3 IP network connectivity issues

Phenomenon: Cannot log in to the web administrator interface.

Solution:

1. Connect the handset to the FXS port and take off the handset to dial##Listen to the network parameters of the device to see if they are correct;
2. Check the LAN where the device is located;
3. Check the connection from the LAN to the device.

3.4 Analog extension not ringing

Phenomenon: The phone does not ring when an incoming call comes in.

Solution:

1. Determine whether the ringing function of the original telephone is normal by replacing the telephone.
2. Click Extension >Analog Extension>Advanced, try to change the number display transmission mode, and dial the extension until the device matches the incoming display mode supported by the phone and rings normally.
3. Go to Grading Settings>Analog Extension>Advanced, change the ringing frequency to a different value to test whether the extension is ringing or not, recommended test values: 15, 20, 30, 40, 50.

 Copyright © Redstone Systems, Inc

3.5 Wrong date displayed on the phone's caller ID

Phenomenon: The date and time displayed on the phone during an incoming call does not match the device.

Solution:

1. Check if you can get the time from a time server on the Internet;
2. If the device cannot access the Internet time server, you can select a computer on the LAN as the time server. If you are using Windows vista/Windows 7/Windows server 2008 operating system, you need to enable Windows Time service manually;
3. Check if the firewall that comes with Windows is enabled on your computer. If the firewall is turned on, follow the steps below to open the port on the firewall for the device to access the time server:
   a) Open the firewall window and click on "Exceptions > Add Port";
   b) Add port 1. Name: ntp-tcp, port number: 123, select TCP method;
   c) Add port 2. Name: ntp-udp, port number: 123, select UDP method;
   d) Verify that the Windows Time service in the Control Panel>Administrative Tools>Services screen is started.
4. After any extension A dials extension B, extension B will display the same time as the device.

 Copyright © Redstone Systems, Inc

3.6 Extension Volume Small

Phenomenon: It feels like the other party is speaking in a low voice during a call.

Solution:

Table 3-2 Extension call volume is low solution

Extension type	Cure
Analog extensions hear low volume	Click ExtensionSettings>Analog Extension>Advanced to increase the gain parameter.
Analog extension dials IP extension, IP extension hears low volume	Click Extension Settings>Analog Extension>Advancedto turn up the Gain to IP parameter.
Incoming caller connects to the IP extension and the IP extension hears low volume.	Click Outside Line Setup>Analog OutsideLine>Advanced and turn up the Gain to IP parameter.

3.7 Analog extension crosstalk

Phenomenon: Calls from other extensions are heard during the call.

Solution:

Usually caused by a short circuit in the telephone line, you need to check the connection of the FXS port and troubleshoot the line.

3.8 Availability of the R key on analog extensions

Pressing theRkey after taking the phone off the hook is logically equivalent to tapping a forked spring, but it is not always reliable in use due to differences in the design standards ofthe Rkeys on different phones. It is recommended that you use**as much as possible when using features such as three-way calling, call forwarding, and call parking.

 Copyright © Redstone Systems, Inc

3.9 Forgetting to customize whitelist results in not being able to log in to the device

REX provides factory built-in whitelist address "192.168.2.100". When you forget the customized whitelist IP address when the whitelist function is on, you can recover it by the following steps.

1. Connect the PC and REX directly with a network cable.
2. Set the IP address of the REX to the same network segment as the built-in whitelist, e.g. 192.168.2.101, via the *90 function key. Operation mode: After taking off the phone, dial *90192*168*2*101#255*255*255*0#192*168*2*1#0# consecutively, and hang up the phone when you hear "successful business registration".
3. Reboot REX.
4. Set the PC's address to 192.168.2.100, You can access it by entering REX's newly set IP address in your PC's browser or SSH client.

3.10 Analog Outbound Inbound and Outbound Abnormalities

Phenomenon: The analog outside line is connected, but the call-in or call-out is abnormal, for example, unable to call in and out, ringing once and then cut off.

Solution:

Check the wiring status of the analog external line in thestatuspage, if there is a "cable abnormality" status, it indicates that the external feed voltage is too low (the standard voltage is 30V), please rewire or coordinate with the operator to solve the problem.

 Copyright © Redstone Systems, Inc

4 OpenVPN Certificate Creation(REX20/REX50)

The device needs to upload a certificate when it is used as an OpenVPN client, and the steps for creating the certificate file are as follows.

Step 1 Get the .ovpn file, or "ca.crt", "client.crt", "client.key" and other information from the VPN server, "ca.crt", "client.crt", "client.key", "ta.key" and other information.

Step 2 Open the .ovpn file with Notepad, or create a new .txt file, noting that the filename must be client.ovpn.

Step 3 Check or supplement what's in the document.

The file contains the following content, the black content is fixed and the orange content is replaced according to the comments.

```
# Affirm that this device is a client
client
# Fill in tap or tun as required by the VPN server
dev tap
persist-tun
persist-key
# For enabling TLS encryption
cipher AES-128-CBC
tls-client
tls-auth ta.key 1
# Fill in the IP address and port of the VPN server here
remote 192.168.143.235 1194
# Fill in tcp or udp as required by the VPN server.
proto udp
tls-remote yfadmin
comp-lzo
passtos
ns-cert-type server
<ca>
# The following is copied from the ca.crt file and replaced. Note that the two lines starting with -----BEGIN and -----END also need to be included.
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
```

 Copyright © Redstone Systems, Inc

</ca>

<cert>

Description: The following is copied from the client.crt file for replacement. Note that the two lines starting with -----BEGIN and -----END also need to be included.

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

</cert>

<key>

The following is copied from the client.key file and replaced. Note that the two lines starting with -----BEGIN and ending with -----END also need to be included.

-----BEGIN RSA PRIVATE KEY-----

-----END RSA PRIVATE KEY-----

</key>

<tls-auth>

The following is copied from the ta.key file and replaced. Note that the two lines starting with ------BEGIN and -----END also need to be included.

-----BEGIN OpenVPN Static key V1

-----END OpenVPN Static key V1-----

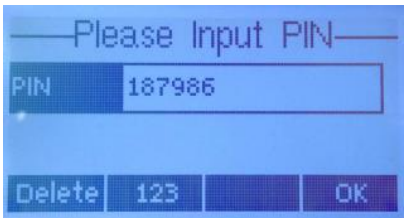
</tls-auth>

Step 4 Save the file when the check or addition is complete. Note that the file name must be client.ovpn. can be uploaded to the device.

 Copyright © Redstone Systems, Inc

Appendix A IP Extension Registration to Devices

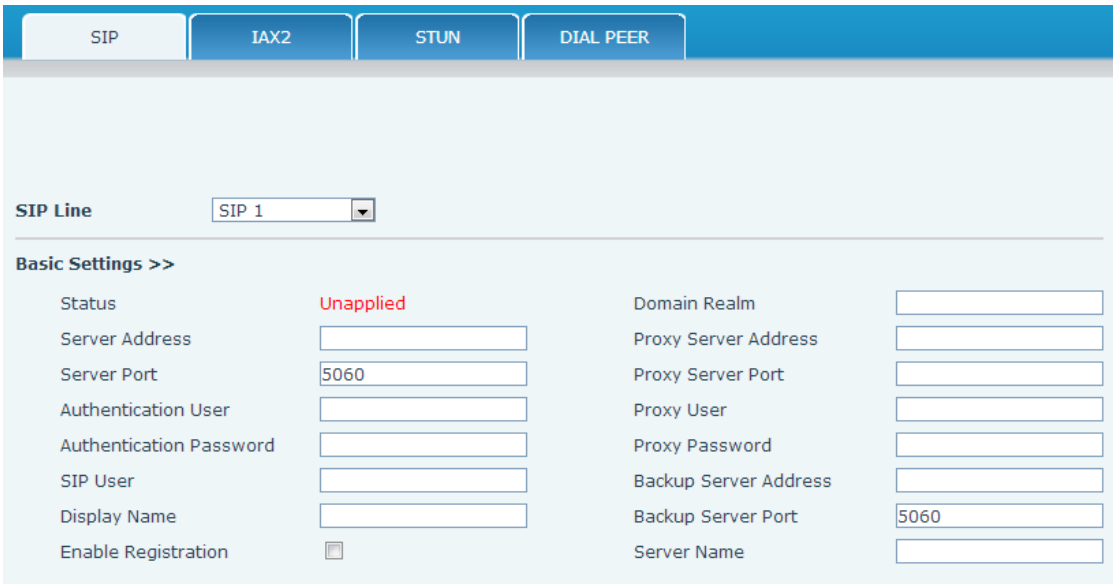
- To use a New Rock NRP phone, enter the PIN of the device's IP extension on the phone when the phone and the device are connected to the network to complete the registration.



- To use a non-NRP series phone, you need to fill in the registration information. The following is an example of the registration information for the NRP1000:

Step 1 Enter the Web management interface of the IP phone, click VOIP > SIP, select the SIP line to be registered, and fill in the registration information in the basic settings.

Figure 4-1 IP Phone Registration Screen



 Copyright © Redstone Systems, Inc

Table 4-1 IP Phone Registration Parameters

Item	Definition
Server address	Fill in the IP address or dynamic domain name of the REX. When the extension needs to register to the REX in the extranet then you need to fill in the extranet access address of the device, which can be viewed in Basic Settings>Extranet Access.
Server port	Fill in the local port of the REX, the default is 5060. Note: The default IP extension registration port of the device is shared with the SIP outside line, both are 5060. This registration port can also be customized in theExtension Settings> IP Extension>Registration Optionsscreen to set it differently from the SIP outside line. Also, the IP extension registration port needs to be modified accordingly.
User ID	Fill in the IP extension account number configured in the REX, such as 208.
Password	Fill in the password corresponding to this extension account number, such as password 187986 for account number 208.
Telephone number	Fill in the IP extension account number configured in the REX, such as 208.
Display name	The name displayed on the other party's phone during a call. The name of the extension user can be set. If not set, the user name is displayed on the other phone, e.g. 208.

Step 2 Check the boxto turn on registrationandsubmit.

Step 3 In the web interface of REX, click Extension >IP Extension to view the IP extension registration status.



It is recommended that IP telephony use G.729 voice coding, with DTMF processing modes and devices that are consistent.

 Copyright © Redstone Systems, Inc

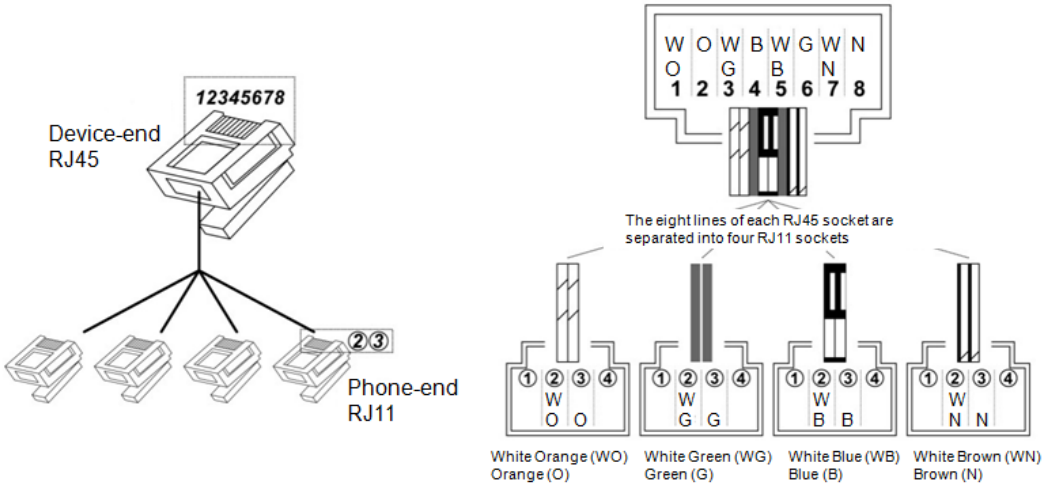
Appendix B RJ45 and RJ11 Line Correspondence Table

Each RJ45 socket has 8 pins and leads to 4 pairs of analog phone lines/trunks according to the Ethernet port pair specification, the correspondence is shown in the table below. Use Category 5 Ethernet cable to connect the interface board to the patch panel when installing the unit. A standard RJ11 telephone cable can also be plugged into the RJ45 socket, where the telephone line/trunk is connected to the third pair of pins and can be used for simple call testing.

Table 4-2 RJ45 Socket Pin Leader Specification

Crystal Head Lead Number	1	2	3	4	5	6	7	8
corresponding user line	first route		second road	third road		second road	fourth road	
	TIP1	RING1	TIP2	TIP3	RING3	RING2	TIP4	RING4
Reference Color	blood orange	orange (color)	light green	indigo plant	indigo	green	white palm	coir (coconut fiber)

Figure 4-2 RJ45 user cable connection diagram



 Copyright © Redstone Systems, Inc