RSBC100 Session Border Controller

Administrator's Manual

Document version: 2025-01

Published: 2025-01-24

Redstone Systems

Copyright © 2025 Redstone Systems, Inc. All Rights Reserved.
All or part of this document may not be excerpted, reproduced and transmitted in any form or by any means without prior written permission from the company.

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

Tel：4259006090

Mail：globalmarketing@redstonesystems.com

1 Contents

1 CONTENTS 1
CONTENTS OF FIGURES 5
CONTENTS OF TABLES 8
2 ABOUT THIS DOCUMENT 10
3 APPLICATION SCENARIOS 11
4 NETWORK TOPOLOGY 14
5 PRODUCT SPECIFICATIONS 15
5.1 PRODUCT OVERVIEW 16
5.2 FUNCTIONS AND APPLICATIONS 16
5.2.1 Functional Features 16
5.2.2 Functional Module 19
5.2.2.1 Call Processing Module 19
5.2.2.2 Safety Module 20
5.2.2.3 Management Module 21
5.3 NORM 22
5.3.1 Performance Parameters 22
5.3.2 Hardware Specifications 23
5.3.2.1 Basic Specification 24
5.3.2.2 Physical and Mechanical Specifications 25
5.3.2.3 Front Panel Component Description 25
5.3.2.4 Rear Panel Component Description 26
5.3.3 Management and Monitoring 26
5.3.3.1 Management Tools 26
5.3.3.2 Remote Management 27
6 HARDWARE INSTALLATION 28

 Copyright © Redstone Systems, Inc

6.1 PRODUCT DESCRIPTION 28
6.1.1 Service 28
6.1.2 characterization 28
6.1.3 Norm 29
6.2 ELECTRICAL SAFETY 29
6.3 SITE PREPARATION 30
6.3.1 Rack Warning 30
6.3.2 Space Requirements 30
6.3.3 Airflow Requirements 31
6.3.4 Temperature Requirement 31
6.3.5 Humidity Requirements 31
6.3.6 Electromagnetic Environment 31
6.3.7 Power Requirements 32
6.3.8 Storage Environment 32
6.4 UNDERSTANDING THE RSBC100 32
6.4.1 Equipment Component 32
6.5 INSTALLATION STEPS 34
6.5.1 Rack Mounting 35
6.5.2 Desktop Installation 36
6.6 CABLING AND CONNECTIONS 36
6.6.1 Network Connection 37
6.6.2 Power Connection 37
6.7 UNINSTALL RSBC100 37
6.7.1 Unloading the RSBC100 in a rack 37
6.7.2 Uninstall the RSBC100 from the desktop 38
6.8 VERIFY INSTALLATION 38
7 CONFIGURING THE RSBC ADMINISTRATOR BACKEND 39
7.1 OPERATOR GROUP 39
7.1.1 IP certification 40
7.1.2 User Name/Password Authentication 45

 Copyright © Redstone Systems, Inc

7.2 PBX 48
7.3 DOMAIN MANAGEMENT 51
7.4 INBOUND SIGNALING (COMPUTING) 53
7.4.1 Number Routing 53
7.4.2 Domain Name Routing 54
7.5 ROUTING (FOR CALLSIGN) 54
7.5.1 Number Routing 54
7.5.2 Domain Name Routing 55
7.6 CALL TRACKING 56
7.7 NETWORK MANAGEMENT 57
7.7.1 Network Setup 57
7.7.2 Port Configuration 60
7.8 TERMINAL RECORDS 62
7.9 CALL RECORD 62
7.10 TEMPLATE MANAGEMENT 63
7.10.1 Call black and white list templates 63
7.10.2 DTMF Templates 64
7.10.3 Call Frequency Templates 65
7.10.4 Media Codec Templates 66
7.10.5 Routing Effective Time Template 67
7.10.6 Number Change Template 68
7.11 APPLICATION CONFIGURATION 69
7.11.1 SIP Configuration 69
7.11.2 Media Configuration 70
7.11.3 Call Configuration 71
7.11.4 Call Black/White List 73
7.12 SECURITY MANAGEMENT 74
7.12.1 WEB Defense 74
7.12.2 SSH Defense 75
7.12.3 SIP Defense 76

 Copyright © Redstone Systems, Inc

7.12.4 Other Defenses 77
7.12.5 Access to black and white lists 77
7.13 SYSTEM MANAGEMENT 78
7.13.1 System Configuration 78
7.13.2 Log Management 78
7.13.3 Backup and Recovery 79
7.13.4 Packetization 80
7.13.5 Operation Log 81
7.13.6 Alarm Log 81
8 GLOSSARY 82

 Copyright © Redstone Systems, Inc

Contents of Figures

Figure1 RSBC100 Application Scenarios Figure 1 11
Figure2 RSBC100 Application Scenarios Figure 2 12
Figure3 RSBC100 Application Scenario Figure 3 13
Figure4 RSBC100 networking topology 14
Figure5 RSBC100 Front view 15
Figure6 RSBC100 Reverse View 15
Figure7 Identifies the location of the interfaces and indicators 26
Figure8 RSBC100 Rear Panel Diagram Identifies the location of each connector and fan 26
Figure9 RSBC100 device front panel illustration 34
Figure10 RSBC100 device back panel illustration 34
Figure11 RSBC Backend Login Screen 39
Figure12 IP Authentication Interface 40
Figure13 Fill in the group name 41
Figure14 Edit Operator Group 41
Figure15 Adding Operator Group Details 42
Figure16 Delete Endpoints 44
Figure17 Refresh Node 44
Figure18 Filtering Users 45
Figure19 Selecting an Outgoing Interface 45
Figure20 Download Template 46
Figure21 Bulk Modify/Delete Username Password Authentication 46
Figure22 Filtering the PBX 48
Figure23 Add PBX Details 48
Figure24 Add PBX Details 2 48
Figure25 New Endpoints 49

 Copyright © Redstone Systems, Inc

Figure26 refreshes the list 51
Figure27 Filter list by type 51
Figure28 Edit/Delete Endpoint Information 51
Figure29 New Domain 52
Figure30 Filter Fields 52
Figure31 number routing 53
Figure32 Domain Name Routing 54
Figure33 Number Routing 54
Figure34 Edit/Delete 55
Figure35 Adding a Domain Route 55
Figure36 Call Tracking 56
Figure37 Reserved Timing Configuration 57
Figure38 Network Settings 58
Figure39 Network Setup 2 59
Figure40 New listening port 60
Figure41 encryption algorithm 61
Figure42 Terminal Records 62
Figure43 Call Log 62
Figure44 New Template 63
Figure45 New DTMF template 64
Figure46 Call Frequency Template 65
Figure47 Media Codec Template 66
Figure48 Routing Effective Time Template 67
Figure49 Number Change Template 68
Figure50 SIP Configuration 69
Figure51 Media Configuration 70
Figure52 Call Configuration 71
Figure53 Call Black/White List 73
Figure54 WEB DEFENSE 74
Figure55 SSH Defense 75

 Copyright © Redstone Systems, Inc

Figure56 SIP Defense 76
Figure57 Other defenses 77
Figure58 Accessing the Black and White List 77
Figure59 System Configuration 78
Figure60 Log Management 78
Figure 61 Historical System Log/Call Log 79
Figure62 Backup and Recovery 80
Figure63 Data Grab Bag 80
Figure64 Operation Log 81
Figure65 Alarm Log 81

 Copyright © Redstone Systems, Inc

Contents of Tables

Table1 RSBC100 Performance Parameters 22
Table2 Supported Codecs 23
Table3 RSBC100 Basic Specifications 24
Table4 Physical and Mechanical Specifications 25
Table5 Front Panel Component Description 25
Table6 Rear Panel Component Description 26
Tables7 Management Tools 26
Table8 Physical Specifications 29
Table9 Electrical Specifications 29
Table10 Environmental Specifications 29
Table11 Items included in the package 32
Table12 Device Front Panel Components 33
Table13 IP Certification 43
Table14 Add Username/Password Authentication 46
Table15 New PBX 49
Table16 New Endpoints 49
Table17 New field 52
Table18 Number Routing 53
Table19 Domain Name Routing 54
Table20 Number Routing 55
Table21 Add Domain Routing 56
Table22 Call Tracking 56
Table23 Network Settings 58
Table24 Network Settings 59
Table25 Port Configuration 60

 Copyright © Redstone Systems, Inc

Table26 Global Configuration 61
Table27 Encryption Algorithm 61
Table28 Call Log 62
Table29 New Template 63
Table30 New DTMF template 64
Table31 Call Frequency Template 65
Table32 Media Codec Template 66
Table33 Routing Effective Time Template 67
Table34 Change of Number Template 68
Table35 SIP Configuration 69
Table36 Media Configuration 70
Table37 Call Configuration 71
Table38 Call Black/White List 73
Table39 WEB DEFENSE 74
Table40 SSH Defense 75
Table41 SIP Defense 76
Table42 Other Defense 77
Table43 Access to Black and White Lists 78
Table44 Log Levels 79
Table45 Backup and Recovery 80

 Copyright © Redstone Systems, Inc

2 About this Document

This manual is designed to provide detailed parameter descriptions and operating instructions for administrators who use and manage the RSBC100 session border controller. It includes technical descriptions of the RSBC100, installation procedures, configuration instructions, maintenance strategies, and solutions to common problems.

 Copyright © Redstone Systems, Inc

3 Application Scenarios

In enterprise communications, common application scenarios include interconnection between enterprise headquarters and branch offices, interconnection between enterprises and carriers, and interconnection between multiple types of communication plat Tables. In these scenarios, the problem of inconsistent protocols and codecs is often encountered. the RSBC100 Session Border Controller (SBC) is compatible with the mainstream signaling and media protocols in the market today, and is able to eliminate the differences between different manufacturers, solutions, and networks, helping enterprises realize seamless converged communications.

Figure 1 Illustrates the problem of protocol and codec inconsistency often encountered when interconnecting enterprise headquarters and branch offices, interconnecting companies and carriers, and interconnecting multiple types of communication platforms. The RSBC100 Session Border Controllers (SBC) are compatible with mainstream signaling and media protocols in the market today, and are capable of eliminating the differences between different manufacturers, different solutions, and different networks, helping enterprises to realize converged communications.

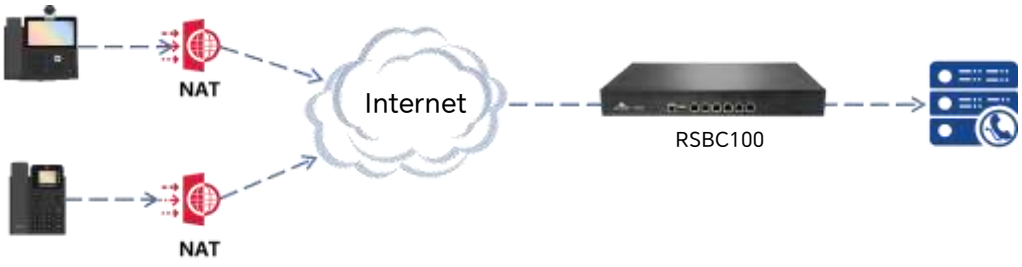


Figure1 RSBC100 Application Scenarios Figure 1

 Copyright © Redstone Systems, Inc

Figure 2 Illustrates that in some particular industries or businesses (e.g., the financial industry), efficient communication is required to be maintained among functional units or subsidiaries. However, the networks of these functional units or subsidiaries are usually independent and are non-trusted networks with each other. When interconnecting, issues such as network topology concealment, media aggregation and forwarding, and security must be considered. the RSBC100 Session Border Controller (SBC) is able to effectively deal with the security issues brought about by untrusted network interconnection in this scenario, ensuring secure and stable communications.

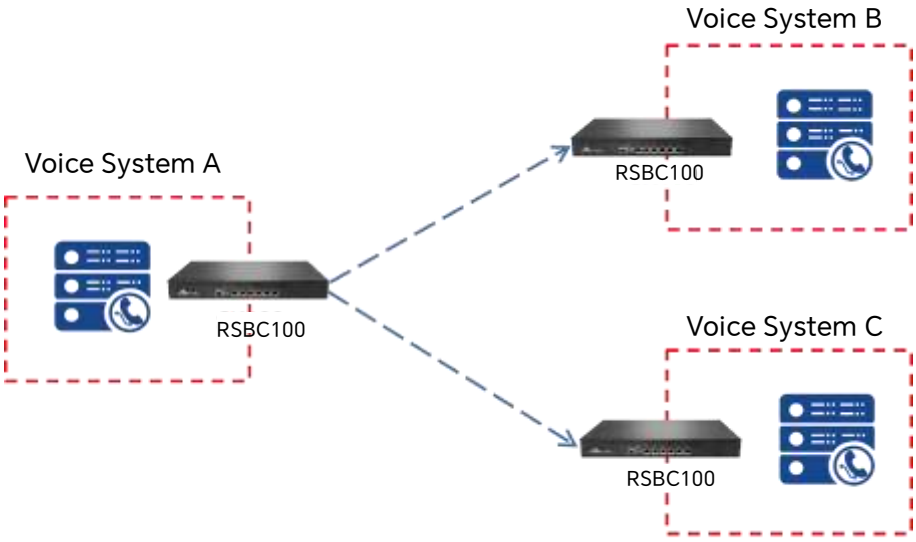


Figure2 RSBC100 Application Scenarios Figure 2

Figure 3 Illustrates that for some enterprises, there may be devices from multiple vendors. In the SIP protocol environment, although the protocol itself has flexibility and business scalability, it also leads to possible incompatibility between the devices of various vendors. RSBC100 can effectively adapt to the devices of different vendors in such scenarios to ensure efficient compatibility and organic integration of multi-vendor equipment environment.

 Copyright © Redstone Systems, Inc

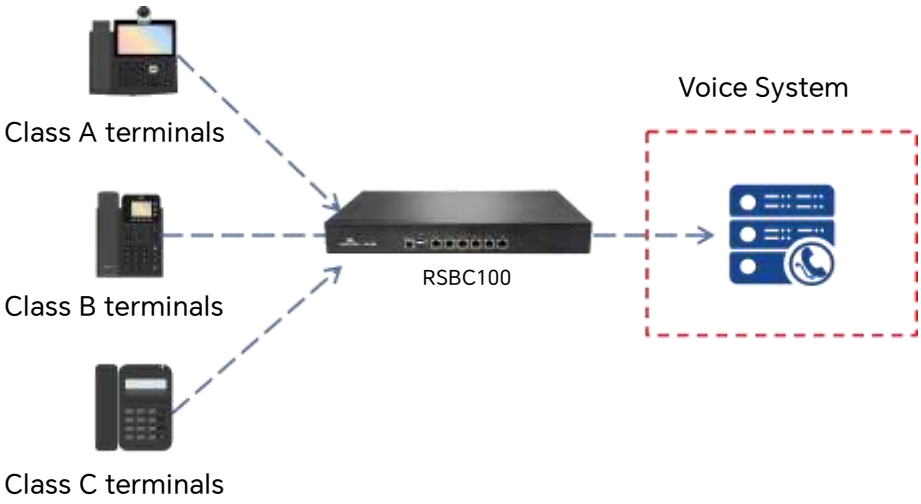


Figure3 RSBC100 Application Scenario Figure 3

 Copyright © Redstone Systems, Inc

4 Network Topology

Figure 4 illustrates a typical networking topology for the RSBC100 session border controller in an enterprise network. This topology includes the internal communication system, the RSBC100 session border controller, and the external communication system.

The topology map includes the following components:

- Internal Communication System: On the left, the RSBC100 connects to internal IP phones and servers within the organization, ensuring secure and efficient internal communications.
- RSBC100 Session Border Controller: In the middle of the diagram, it serves as a bridge between the internal network of the enterprise and the external network, ensuring the security and reliability of data transmission.
- External Communication System: On the right, the RSBC100 connects to the IP Multimedia Subsystem (IMS) of an Internet Service Provider (ITSP), which supports a variety of voice and video coding standards (e.g., G.723 .1, G.729a/b, iLBC, G.722, G.722.1, G.722.2, AMR, OPUS, H.264, and H.265) to interoperate with external networks.

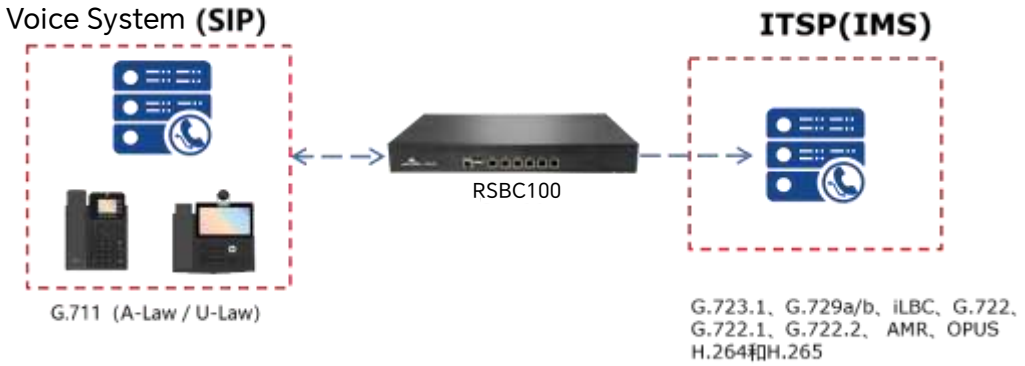


Figure4 RSBC100 networking topology

 Copyright © Redstone Systems, Inc

5 Product Specifications

Performance and reliability are key factors when selecting and deploying enterprise communications equipment. The RSBC100 Session Border Controller delivers high performance and flexibility with a variety of advanced features to meet the needs of small and medium-sized businesses. The devices support multi-user concurrent sessions and provide high-quality voice and video communications. By utilizing advanced encryption and security measures, the RSBC100 ensures the confidentiality and integrity of communications. In addition, a user-friendly management interface simplifies daily operation and maintenance.



Figure5 RSBC100 Front view



Figure6 RSBC100 Reverse View

 Copyright © Redstone Systems, Inc

5.1 Product Overview

Designed for small and medium-sized businesses, the RSBC100 Session Border Controllers provide a high-performance and highly reliable communications solution. By supporting multi-user concurrent sessions and high-quality voice and video communications, the RSBC100 meets the needs of enterprises in mobile office, branch interconnection and multi-network convergence. It is marketed as a secure, stable and easy-to-manage communication platform for small and medium-sized enterprises to ensure efficient internal and external communication.

5.2 Functions and Applications

This section provides a detailed description of the features of the RSBC100 Session Border Controllers and their applicability in different application scenarios. The RSBC100 provides a reliable communication solution for small and medium-sized businesses through its high availability, flexible protocol support, powerful user management capabilities, and security features. The following content includes a detailed description of the functional features, call handling, security measures and management and maintenance.

5.2.1 Functional Features

- ✓ Supports dual-machine deployment: Improves the high availability of the system and ensures that when one device fails, the other device can seamlessly take over the work to ensure the continuous operation of the system.
- ✓ Standard Session Initiation Protocol SIP and Flexible Routing Rules: RSBC100 is perfectly compatible with IMS system and supports flexible routing rule settings to adapt to different network environments and application scenarios.
- ✓ User Support: The RSBC100 supports up to 1,000 user registrations and is capable of handling 120 concurrent sessions and 70 voice media transcoders at the same time, providing powerful communication capabilities for enterprises.
- ✓ Multiple coding standards: The device is compatible with a wide range of voice and video coding standards, including G.711 (A-Law / U-Law), G.723.1, G.729a/b, iLBC, G.722, G.722.1, G.722.2, AMR, H.264, and H.265, ensuring compatibility with different devices and

 Copyright © Redstone Systems, Inc

systems.

- ✓ Voice and Video Calls: Supports high quality voice and video calls to meet the needs of enterprises for multimedia communications.
- ✓ Call Recording: Supports call recording function, which is convenient for enterprises to record and monitor calls.
- ✓ Registration Support: Supports forwarding registration, agent registration and Trunk docking, facilitating integration and interconnection with other communication systems.
- ✓ Transmission Protocol: Supports Session Initiation Protocol SIP transmission based on User Datagram Protocol UDP and Transmission Control Protocol TCP to ensure the stability and reliability of data transmission.
- ✓ Encrypted Sessions: Supports SIP encryption via Transport Layer Security Protocol TLS, as well as Secure Real-Time Transport Protocol SRTP and Datagram Transport Layer Security Protocol DTLS-SRTP encrypted sessions, providing a high level of communication security protection.
- ✓ NAT Penetration: Supports symmetric and asymmetric network address translation NAT penetration and survivability for signaling and media, adapting to the deployment of complex network environments and ensuring the stability of communications.
- ✓ Security mechanism: Support for whitelist and blacklist management, topology hiding, denial-of-service DoS and distributed denial-of-service DDoS (attack defense, and provide voice firewall function to protect the core equipment from attacks.
- ✓ Voice Quality Monitoring: Provides voice quality monitoring function, which can monitor the packet loss rate to ensure the call quality.
- ✓ Call Recording: Support call recording function, convenient for enterprises to record and monitor calls.
- ✓ Management Function: Provide friendly graphical Web operation interface, support remote upgrade and remote maintenance, simplify the daily management of equipment.
- ✓ Enhanced Security: Provides protection mechanisms, DoS, DDoS and UDP/TCP flooding attacks, protects system resources and ensures enterprise network security.
- ✓ Extensive Protocol Support: Supports a wide range of protocols, including: IPv4/IPv6, User Datagram Protocol/Transmission Control Protocol, Real-Time Transport Protocol/Real-

 Copyright © Redstone Systems, Inc

Time Transport Control Protocol, Message Session Relay Protocol, Transport Layer Security Protocol/Secure Real-Time Transport Protocol, Session Initiation Protocol/IP Multimedia Subsystem, Hyper Text Transmission Protocol/Secure Hyper Text Transmission Protocol, Network Time Protocol/Simple Network Time Protocol, Network Time Protocol/Simple Network Time Protocol, with strong compatibility.

- ✓ Comprehensive Function Support: Not only provide session initial protocol SIP and IP multimedia subsystem docking solution, but also support standard session border controller SBC (functions, including branch networking, cross-network interoperability, heterogeneous networking between different communication systems, etc.).
- ✓ Media Processing Functions: Supports customized header fields, codec conversion, protocol conversion, dual-tone multi-frequency DTMF (mode conversion, call recording, voice quality monitoring, trunk redundancy and load balancing, call frequency limitation, and other functions.
- ✓ Protocol compatibility and Interoperability: RSBC100 session border controllers are compatible with the mainstream signaling and media protocols in the market, eliminating the differences between different manufacturers, solutions and networks, and helping enterprises realize unified communications.
- ✓ NGN and IMS Protocol Conversion: The RSBC100 Session Border Controller supports protocol conversion between NGN and IMS systems, which is a next-generation network that handles the interconnection between traditional telephony networks and IP networks, and manages the processing, forwarding, and conversion of media streams to enable the transmission of services such as voice and data across different networks. an architectural framework that provides IP-based multimedia services such as voice, video calls and instant messaging. The RSBC100 devices enable efficient conversion of different signaling protocols (e.g., SIP, H.323) and media protocols between NGN and IMS, ensuring the stability and compatibility of voice and data communications in different network environments, and providing a seamless user experience.
- ✓ Terminal Proxy/Forwarding Registration and Authentication: RSBC100 devices support proxy registration and forwarding registration functions for terminal devices, ensuring that terminal devices are authenticated and registered in different network environments.

 Copyright © Redstone Systems, Inc

Through the proxy or forwarding method, terminal devices can flexibly access various networks, improving the compatibility and stability of the network.

- ✓ SIP B2BUA (Back-to-Back User Agent): Supports SIP (SIP, Session Initiation Protocol) B2BUA function, which acts as an intermediary between two SIP sessions, processes and modifies SIP messages, and realizes call control and session management.
- ✓ Signaling Message Slicing: Support signaling message slicing function, through the large size of the signaling message is divided into smaller segments for transmission, to avoid transmission failure or delay caused by a single message is too large, so as to improve the overall efficiency and stability of signaling transmission.

5.2.2 Functional Module

The RSBC100 Session Border Controller provides a flexible and efficient communications solution for small and medium-sized businesses through its advanced feature modules. The following section details the specific features of key modules such as call handling, security and management.

5.2.2.1 Call Processing Module

The Call Handling module is responsible for managing and optimizing all call routing and handling processes. Its main functions include:

- Call Routing: Supports routing based on calling and called number prefixes, allowing flexible call path settings to accommodate different network structures and needs.
- Time slot policy: Support selecting call routing according to the preset time slot policy, realizing different call handling methods for working hours and non-working hours.
- Trunk Redundancy and Load Balancing: Supports redundancy and load balancing of trunk lines to ensure automatic switching to a backup line in the event of a line failure, while optimizing call distribution to prevent overload.
- Heterogeneous networking: Support heterogeneous networking routing redundancy and backup and load balancing. Connections between different types of communication systems and devices can realize interconnection and interoperability between different network environments and devices by means of routing redundancy and backup and load balancing.

 Copyright © Redstone Systems, Inc

5.2.2.2 Safety Module

The security module is responsible for ensuring data security and network protection during communication. Its main functions include:

- Access Control: Use blacklist and whitelist mechanisms to control access to devices and network resources to ensure that only authorized users have access.
- Attack Defense: Provides defense mechanisms to protect against a wide range of attacks, including:
  - Denial of Service Attack DoS: Prevents malicious users from exhausting system resources by sending a large number of requests.
  - Distributed Denial of Service Attacks DDoS: Defend against attacks from multiple sources and protect systems from distributed attacks.
  - UDP/TCP Flood Attack (Flood): prevents attacks that cause network congestion and resource exhaustion by sending large numbers of UDP or TCP packets.
- SIP Attack Defense: A policy-based Session Initiation Protocol SIP attack defense mechanism that detects and blocks malicious SIP traffic to protect communication security.
- Encrypted Sessions: provides a variety of encryption mechanisms to secure sessions, including:
  - Transport Layer Security Protocol TLS: Prevents data from being intercepted and tampered with in transit by encrypting transport layer data.
  - Secure real-time transmission protocol: encrypts real-time audio and video data to ensure the security of real-time communication.
  - Datagram Transport Layer Security Protocol DTLS-SRTP (DTLS, Datagram Transport Layer Security): Combines DTLS and SRTP to provide enhanced real-time data encryption to ensure the security of datagram transmission.
- Call Frequency Restriction: Based on the preset policy, it restricts the number of calls per unit of time to prevent the abuse and attack of system resources by abnormal traffic.
- Disaster-tolerant deployment: Support local dual-machine disaster-tolerant deployment, through dual-machine hot backup to ensure that when one device fails, the other device can seamlessly take over to ensure business continuity and reliability.

 Copyright © Redstone Systems, Inc

5.2.2.3 Management Module

The Management Module provides tools and features to simplify and optimize equipment management and maintenance. Its key features include:

- Management Interface: Provides a Web-based management interface that supports both Simplified Chinese and English languages. Administrators can access the device through a browser for configuration and maintenance.
- Command Line Management: Supports command line interface (CLI) management via SSH (Secure Shell), a secure shell protocol. Administrators can use SSH to access the device and perform advanced configuration and maintenance operations via CLI for scenarios requiring fine-grained control.
- Configuration Management: Supports backup and recovery of configuration data. Administrators can save the current configuration on the device and restore to the previous configuration state when needed to ensure the security and reliability of configuration changes, and all operations are completed on the current device.
- Network Data Capture: Built-in network data capture feature allows administrators to capture and analyze network packets. This feature is useful for troubleshooting network problems, analyzing traffic and performing security checks.
- Log Management: Provides multi-level log management functions, including system log, operation log and call log. Administrators can view and analyze the logs to understand the device's operational status, configuration change records and call activities for troubleshooting and performance optimization.
    - Syslog: records system-level events and status information for the device.
    - Operation Log: Records all operations performed by the administrator on the device.
    - Call Log: Records detailed information on all call activity, including call time, duration, and participants.

 Copyright © Redstone Systems, Inc

5.3 Norm

This section describes in detail the various specification parameters of the RSBC100 Session Border Controller. It covers the performance specifications of the device, network protocol support, transmission capabilities, quality of service control, and voice and video processing capabilities. This information provides a comprehensive understanding of the performance and application capabilities of the RSBC100 and serves as a reference for configuration and deployment.

5.3.1 Performance Parameters

Table1 RSBC100 Performance Parameters

Performance Indicators	Descriptive
Maximum number of concurrent sessions	120 (unencrypted) / 100 (encrypted) concurrent routes
Maximum number of codec conversions	Route 70
Call processing power (CPS)	20 calls per second
Number of user registrations	Supports up to 1000 registered users
Support for coding standards	G.711 (A-Law / U-Law), G.723.1, G.729a/b, iLBC, G.722, G.722.1, G.722.2, AMR, H.264, H.265
Quality of Service (QoS)	802.1p/Q VLAN tagging, IP TOS (Type of Service), Differentiated Services (DiffServ)
Voice Gain Control	Fixed/dynamic voice gain control
Jitter Buffer	be in favor of
Fax Support	G.711 transmissible fax, T.38 fax, compatible with class G3 fax machines, up to 33.6 kbps (transmissible)
Dual-tone multi-frequency DTMF mode	rfc2833, sip-info, inband
network protocol	IPv4/IPv6, SSH, HTTP/HTTPS, DNS, ARP, NTP/SNTP, ICMP
transportation protocol	UDP/TCP, RTP/RTCP/MSRP, TLS/SRTP

 Copyright © Redstone Systems, Inc

Table2 Supported Codecs

Codec type	Supported Codecs	Descriptive
Audio Codec	G.711 (A-Law / U-Law)	High fidelity audio, commonly used in traditional telephone systems.
	G.723.1	High compression ratio audio codec for low bandwidth environments.
	G.729a/b	Efficient voice codec for bandwidth-constrained networks
	iLBC	Internet low-bandwidth codec for voice transmission in unstable network environments.
	G.722	Wideband audio codec for higher sound quality.
	G.722.1	Improved wideband audio codec for conference systems.
	G.722.2	Broadcast-quality audio codec for high-definition voice communications.
	AMR	Adaptive multirate codecs, commonly used in mobile communication systems.
Video Codec	H.264	Widely used HD video codec for a wide range of video communication applications.
	H.265	Higher compression efficiency video codec for UHD video transmission.

5.3.2 Hardware Specifications

This section provides detailed hardware specifications for the RSBC100 session border controller. It covers the basic hardware configuration of the device, physical and mechanical specifications, and descriptions of front and rear panel components. This information helps users understand the hardware performance, interface configuration, and installation requirements of the device and provides guidance for deployment and maintenance.

 Copyright © Redstone Systems, Inc

5.3.2.1 Basic Specification

Table3 RSBC100 Basic Specifications

Name	Norm	Descriptive
Processor (CPU)	2.60GHz mains frequency	High-performance processor to ensure fast data processing and system response.
system memory	8GB	Sufficient memory capacity to support multitasking and stable operation.
system storage	250GB	Large storage capacity for storing system data and logs.
network port	6 x 10/100/1000Mbps Adaptive Ethernet port	Adaptive Ethernet ports, supporting multiple rates (10Mbps, 100Mbps, 1000Mbps), are able to automatically adjust to the rate of network devices to ensure optimal performance.
Chassis Size (L x W x H)	430mm × 300mm × 45mm	Size chassis for a variety of installation environments.
power supply	100 to 240 volts. 50/60 Hz. 1A	Compatible with electrical standards in different regions of the world.
working environment	Temperature: -15 to 60℃ . Relative humidity: 10% to 90% (non-condensing)	Adapt to extreme working environment to ensure stable operation of equipment.
Storage environment	Temperature: -40 to 70℃ . Relative humidity: 5% to 90% (non-condensing)	Ensure that the equipment is kept undamaged for long periods of time.
power wastage	50W	The power consumption of a device under normal operating conditions.
Certifications and standards	CQC	International and national standards and certifications to which the equipment conforms

 Copyright © Redstone Systems, Inc

5.3.2.2 Physical and Mechanical Specifications

Table4 Physical and Mechanical Specifications

Norm	Descriptive
weights	3.7kg
connector	Six 10/100/1000Mbps adaptive network ports; 2 USB ports (not yet enabled); 1 CONSOLE port (not enabled yet); 1 VGA port (not yet enabled)
cooling system	2 fans
power supply	Standard power connector with switch
Power connector	250V fuse only
Installation	Rack mounting and tabletop placement

5.3.2.3 Front Panel Component Description

Table5 Front Panel Component Description

port name	typology	descriptive
CONSOLE	RJ45	1 CONSOLE
USB	USB 3.0	2 USB ports
ETH0	RJ45	10/100/1000Mbps Adaptive Ethernet port
ETH1	RJ45	10/100/1000Mbps Adaptive Ethernet port
ETH2	RJ45	10/100/1000Mbps Adaptive Ethernet port
ETH3	RJ45	10/100/1000Mbps Adaptive Ethernet port
ETH4	RJ45	10/100/1000Mbps Adaptive Ethernet port
ETH5	RJ45	10/100/1000Mbps Adaptive Ethernet port
PWR indicator	LED	Power indicator
HDD indicator	LED	Hard disk indicator

 Copyright © Redstone Systems, Inc



Figure7 Identifies the location of the interfaces and indicators

5.3.2.4 Rear Panel Component Description

Table6 Rear Panel Component Description

port name	typology	descriptive
VGA	DB-15	VGA connector
POWER	IEC C14	Power connector with switch
fan (loanword)	internally installed	Used for internal heat dissipation of equipment to keep the temperature of the equipment stable



Figure8 RSBC100 Rear Panel Diagram Identifies the location of each connector and fan

5.3.3 Management and Monitoring

This section describes the management and monitoring tools for the RSBC100 Session Border Controller, as well as the remote management features and how to use them.

5.3.3.1 Management Tools

Tables7 Management Tools

Item	Definition
CLI command	Access via Secure Shell Protocol (SSH) provides advanced configuration and maintenance operations for scenarios requiring fine-grained control.
web interface	Web-based management interface supports both Simplified Chinese and English languages. Administrators can access the device through a browser to

 Copyright © Redstone Systems, Inc

	perform configuration, monitoring and maintenance operations. The interface is designed to be intuitive and friendly, suitable for most users.

5.3.3.2 Remote Management

The RSBC100 devices support remote management via a command line interface (CLI) and backend services, enabling administrators to configure and maintain the devices from any location:

- Remote Configuration: Administrators can access the device remotely through the web interface or CLI for configuration management. The remote configuration function allows administrators to make parameter adjustments, policy settings, and feature enable/disable for the device without being on site, improving management efficiency.
- Log Management: Provides multi-level log management functions, including system log, operation log and call log. Administrators can view and analyze the logs to understand the device's operational status, configuration change records and call activities for troubleshooting and performance optimization.

 Copyright © Redstone Systems, Inc

6 Hardware Installation

6.1 Product Description

The RSBC100 Session Border Controller is a high-performance device designed for voice and video communications. It supports SIP, encrypted sessions, NAT penetration, and more to ensure a high-quality communication experience. The device also features high availability, security, and call routing.

6.1.1 Service

The RSBC100 provides the following service interfaces:

- 6 10/100/1000 Base-T Ethernet ports
- 1 CONSOLE interface
- 2 USB ports
- 1 VGA port
- 1 power connector and power switch

6.1.2 characterization

Key features of the RSBC100 include:

- High-performance processing capability: Supports concurrent sessions and large-scale data transmission to enhance system processing efficiency.
- Powerful security features: supports encrypted sessions and multi-layer security protection mechanisms to ensure the security of data transmission.
- Flexible Network Connectivity: Provides multiple 10/100/1000 Base-T Ethernet ports to support multiple network topologies for flexible network configuration.
- High-availability design: supports redundant configurations to ensure high reliability and stability of the equipment and minimize downtime.

 Copyright © Redstone Systems, Inc

6.1.3 Norm

Physical Specifications:

Table8 Physical Specifications

Name	Norm
sizes	430mm (W) x 300mm (D) x 45mm (H)
weights	3.7 kg

Electrical Specifications:

Table9 Electrical Specifications

Name	Norm
Input Power	100 ~ 240V AC, 50/60Hz, 1A
power wastage	50W

Environmental specifications:

Table10 Environmental Specifications

Name	Norm
operating temperature	-15 to 60℃
Operating humidity	10% to 90% (non-condensing)

6.2 Electrical Safety

Follow these electrical safety guidelines when installing and operating the RSBC100 Session Border Controller:

- Be careful when handling energized connections: care must be taken to avoid the risk of electric shock when carrying out any operation while the equipment is energized.
- Avoid humid environments: Do not install and operate electrical equipment in wet or high humidity environments to prevent short circuits and equipment damage.
- Power supply rating: Ensure that the power supply is rated sufficiently to operate the system safely and provide current overload protection.
- POWER CORD PROTECTION: Do not allow any objects to press on the power cord, and do not place the power cord where people will stand or walk on it to prevent abrasion or

 Copyright © Redstone Systems, Inc

damage to the power cord.

- Use a standard power adapter: use the standard power adapter model included in the package, which meets the requirements for safe power supply.

-Do not disassemble the equipment. Do not disassemble the unit: Do not open the unit case without the permission of technical support, as this is dangerous and will void the warranty.

6.3 Site preparation

Before installing the RSBC100 Session Border Controller, proper site preparation must be performed.

Rack Mounting

The RSBC100 can be mounted in any industry-standard (EIA) 19-inch (482.6 mm) 4-post rack using mounting brackets.

6.3.1 Rack Warning

To minimize the risk of personal injury or equipment damage, make sure:

- Adjust the feet at the bottom of the rack to make them firmly touch the ground to ensure that the rack is stable.
- In case of single rack mounting, take measures to increase the stability of the rack, e.g. by installing fixing feet.
- In the case of multiple rack installations, make sure that the racks have been securely attached to each other to improve overall stability.

6.3.2 Space Requirements

The RSBC100 installation requires a 4-post rack with a depth of 300 to 900 mm.

- Sufficient space should be left in front of the rack for installation and maintenance operations: a minimum of 610 mm (24 inches) is recommended.

 Copyright © Redstone Systems, Inc

- Sufficient space should be left at the rear of the rack to ensure good airflow and cable connections: it is recommended to leave at least 760 mm (30 inches).

6.3.3 Airflow Requirements

To ensure proper operation of the RSBC100 and to prevent overheating, follow the recommendations below:

- The installation location should be well ventilated and avoid installation in enclosed spaces.
- The RSBC100 is equipped with 2 fans located on the rear panel of the unit, ensuring that the fan vents are not obstructed.
- The sides of the RSBC100 units are designed with multiple rows of ventilation holes on both sides of the unit, which are similar to a grille shape. They help air circulation and heat dissipation inside the unit. Make sure that these ventilation holes are not blocked to maintain good heat dissipation performance.

6.3.4 Temperature Requirement

To ensure proper operation of the RSBC100, follow the temperature requirements below:

- Operating temperature range: -15 ~ 60℃

6.3.5 Humidity Requirements

To ensure proper operation of the RSBC100, follow the humidity requirements below:

- Relative Humidity Range: 10% ~ 90

6.3.6 Electromagnetic Environment

To ensure proper operation of the RSBC100, follow the electromagnetic environment requirements below:

- The device should be kept away from strong magnetic and electric fields to avoid affecting the normal operation of the device. Strong electromagnetic interference may cause the

 Copyright © Redstone Systems, Inc

device to not work properly or data transmission errors.

6.3.7 Power Requirements

The RSBC100 is equipped with a universal power adapter. To ensure proper operation and safety of the unit, please check the following power requirements before installation:

- Power adapter: Use the power plug included in the package.
- AC Power Input: Ensure that the AC power input meets the specifications indicated on the power adapter, typically 100-240V, 50/60Hz, 1A.

6.3.8 Storage Environment

To ensure that the RSBC100 is not damaged during storage, follow the storage environment requirements below:

- Temperature range: -40 ~ 70°C
- Relative humidity range: 5% ~ 90% (non-condensing)

6.4 Understanding the RSBC100

Before installing the RSBC100 Session Border Controller, it is critical to understand the components of the device and their functions.

6.4.1 Equipment Component

This section describes in detail the main components of the RSBC100 and their functions, including the location and purpose of each interface and indicator.

- Items included in the package:

When unpacking the RSBC100, make sure that the following items are available

Table11 Items included in the package

 Copyright © Redstone Systems, Inc

Item	Definition
crown screw	Multiple for securing equipment and mounting racks.
footrest	4 for secure mounting of the unit to prevent slipping.
lug	2 for mounting the unit in a rack.
Distribution screws for lugs	Multiple pcs for securing lugs and equipment.
power adapter	Provide the power supply required for the equipment.

- Device front panel assembly:

Table12 Device Front Panel Components

Item	Definition
CONSOLE Interface	1 for connection to the console, located on the left side of the front panel of the device. This interface is currently not enabled and may be supported in the future through a software update or other means of providing functionality.
USB interface	Includes 2 USB ports for connecting USB devices, located on the front panel of the unit, immediately to the right of the CONSOLE connector.
Network interface	Includes 6 Ethernet ports (ETH0, ETH1, ETH2, ETH3, ETH4, ETH5) for connecting network devices and transferring data. Located in the center and right side of the front panel of the device.
Functionality	Each port supports Gigabit Ethernet connectivity, providing high-speed data transfer and network connectivity. Ideal for connecting routers, switches and other network devices.
Network Status Indicator	Next to each network interface are corresponding status LEDs to indicate connection status and data transfer status. A green light indicates a normal connection and a yellow light indicates data

 Copyright © Redstone Systems, Inc

	transfer.
Power Supply Indicator (PWR)	Displays whether the device is powered on or not. Green color indicates that the device is powered on and operating normally.
Hard Disk Drive Indicator (HDD)	Displays the operating status of the hard disk. Green indicates that the hard disk is working normally, and blinking indicates that the hard disk is performing read/write operations.



Figure9 RSBC100 device front panel illustration

- Equipment Back Panel Assembly

The back panel of the device is shown in the figure and contains the following components:

- VGA port (not currently enabled): 1 for connecting a monitor. This interface is currently not enabled and may be supported in the future through software updates or other means of providing functionality.
- Cooling fan: 2pcs, used for heat dissipation of the equipment, to ensure that the equipment maintains a suitable temperature during operation.
- Power switch: 1 for powering the unit on and off.
- Power socket: 1 pc for connecting the power cord.



Figure10 RSBC100 device back panel illustration

6.5 Installation Steps

Before installing the RSBC100 Session Border Controller, ensure that the unit is mounted in a location that meets safety and operational requirements. Installation methods include rack

 Copyright © Redstone Systems, Inc

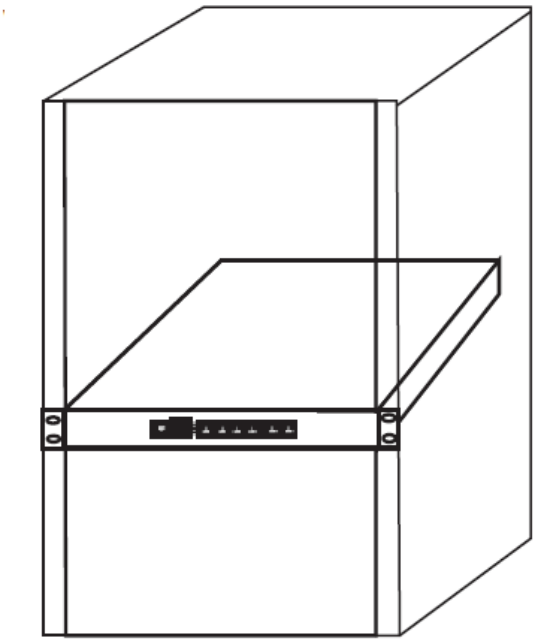
mounting and desktop mounting. Follow the steps below to install the device.

6.5.1 Rack Mounting

1. Open the RSBC100 shipping carton; use caution to avoid cutting the contents. Verify that all package contents are present.

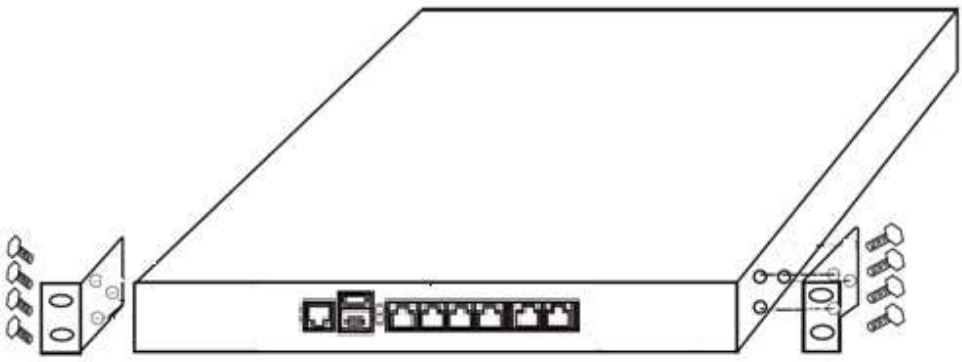
2. Remove the RSBC100 and mounting hardware. Ensure that all necessary parts are present and have not been damaged during transportation.

3. Select 1U of space in the rack to install the RSBC100.



Selection of mounting location

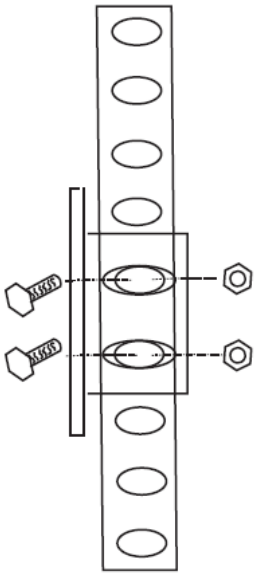
4. Attach each lug to the RSBC100 through the three screw holes.



lug connection

5. Install the RSBC100 into the rack and secure the two lugs to the rack with the four crown

screws.



Fixed mounting lugs

6. Ensure that the RSBC100 power switch is set to OFF (O).

7. Connect the power cord to the power connector of the RSBC100 and plug it into a grounded outlet.

8. Turn on the power switch of the RSBC100 to the (I) position.

6.5.2 Desktop Installation

1. Find a safe and easily accessible mounting location.

2. Place the RSBC100 unit on a tabletop.

3. Make sure the RSBC100 power switch is set to OFF (O).

4. Connect the power cord to the power connector of the RSBC100 and plug it into a properly grounded outlet.

5. Turn on (I) the RSBC100 power switch to ensure that the unit begins normal operation.

6.6 Cabling and Connections

After completing the installation of the RSBC100, network and power connections need to be made. The following are specific wiring and connection steps to ensure that the unit can operate and communicate with network devices.

 Copyright © Redstone Systems, Inc

6.6.1 Network Connection

1. Plugging in the Ethernet cable: Plug the Ethernet cable into the Ethernet ports (ETH0, ETH1, ETH2, ETH3, ETH4, ETH5) on the RSBC100. These ports are used to connect to a router, switch, or other network device to establish a network connection for data transfer and communication.
2. Verify connection status: Check the link LEDs of the corresponding Ethernet ports. Green indicates a normal connection and yellow indicates data transmission. Ensure that all connected ports are in normal operating condition.
3. Repeat steps: Repeat steps 1 and 2 as necessary to connect other network devices. Each port can be independently connected to different devices to realize data communication and network management among multiple devices.
4. Cable organization: Organize cables in accordance with the local practices of the site to ensure that cabling is neat, secure and free from tangled or damaged cables.

6.6.2 Power Connection

1. Connect the power cord to the RSBC100 power connector.
2. Plug the power cord into a grounded outlet.
3. Make sure the power switch is set to OFF (O).
4. Turn on the power switch of the RSBC100 to the (I) position to ensure that the unit begins to operate normally.

6.7 Uninstall RSBC100

You may need to uninstall the RSBC100 when you need to maintain, upgrade, or replace the unit. Be sure to follow the correct steps to avoid damage to the unit or related hardware. The following are detailed steps for uninstalling the device.

6.7.1 Unloading the RSBC100 in a rack

1. Make sure the power switch is set to OFF (O) and disconnect the power cord.
2. Use a screwdriver to loosen the four bolts on the rack lugs and remove the RSBC100 from the rack.

 Copyright © Redstone Systems, Inc

3. Remove the rack lugs, if necessary.

4. Remove the RSBC100 and mounting hardware, ensuring that all necessary components were not damaged during removal.

6.7.2 Uninstall the RSBC100 from the desktop

1. Make sure the power switch is set to OFF (O) and disconnect the power cord.
2. Remove the Ethernet cable and power cord.
3. Remove the RSBC100 from the table.

6.8 Verify Installation

- Check the Power Indicator: Verify that the Power Indicator (PWR) is on, indicating that the unit is powered up.
- Check Ethernet Port Indicators: Make sure the link indicators are lit for all connected Ethernet ports (ETH0, ETH1, ETH2, ETH3, ETH4, ETH5) to ensure proper connectivity.
- Check Fan Operation: Make sure the fan on the back of the unit is operating properly to ensure that the unit is dissipating heat well.
- Logging in to the device: by connecting to the Ethernet interface, ensure that you can access the device's management interface for configuration and management.

 Copyright © Redstone Systems, Inc

7 Configuring the RSBC Administrator Backend

Log in to the RSBC administrator backend

Step.1 Open your browser. Enter the SBC address, example: 192.168.180.134: 5000

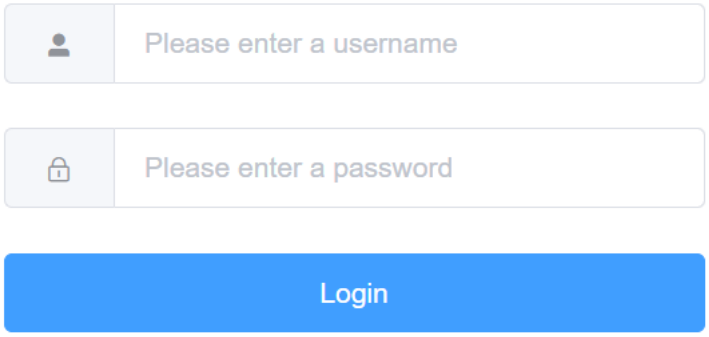


Figure11 RSBC Backend Login Screen

Step.2 Enter the user name and password. User name and password default to admin

7.1 Operator Group

In the management interface of the RSBC, the "Operator Group" section is mainly used to configure and manage the authentication mechanism for connecting with external operators. This section provides management of carrier information, including IP authentication and user name/password authentication. The administrator can add, edit and refresh operator groups in this interface to ensure the correct connection and communication security between the device and the external network.

 Copyright © Redstone Systems, Inc

7.1.1 IP certification

IP authentication verifies the validity of a connection request by matching it with the carrier's preset IP address. The administrator can configure the IP address range of the carrier here.

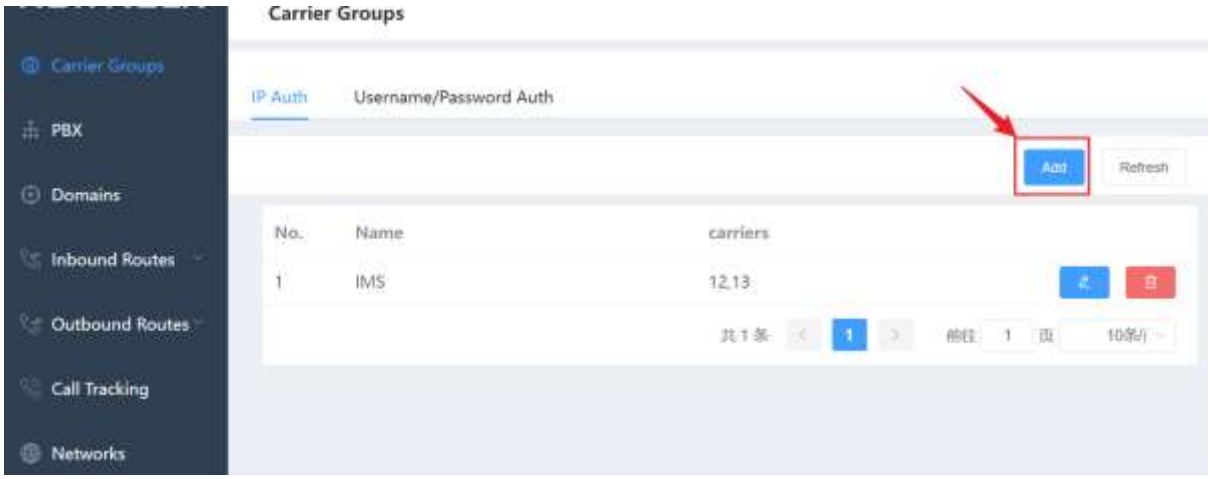
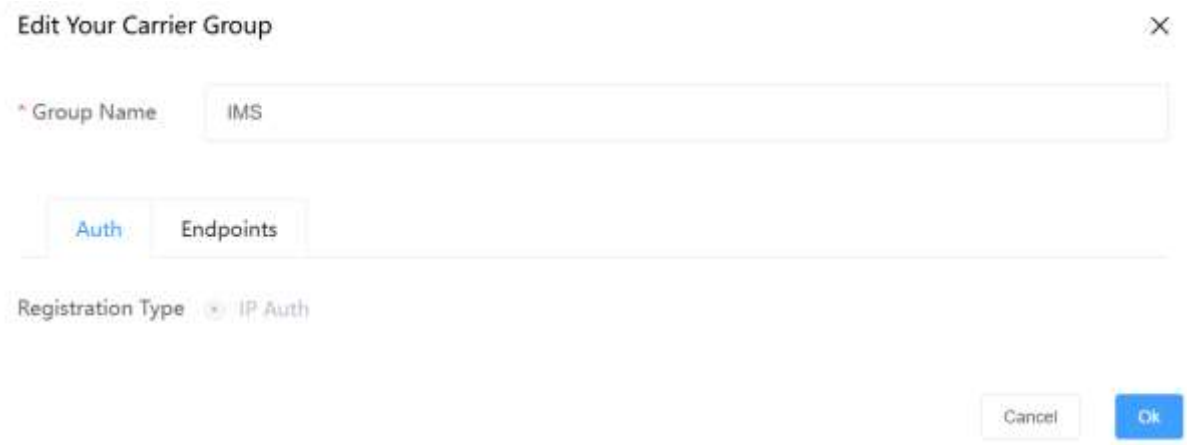


Figure12 IP Authentication Interface

Step.1 Navigate to Carrier Groups > IP Authentication and click Add Configuration Carrier Group.



Step.2 Fill in the group name

 Copyright © Redstone Systems, Inc

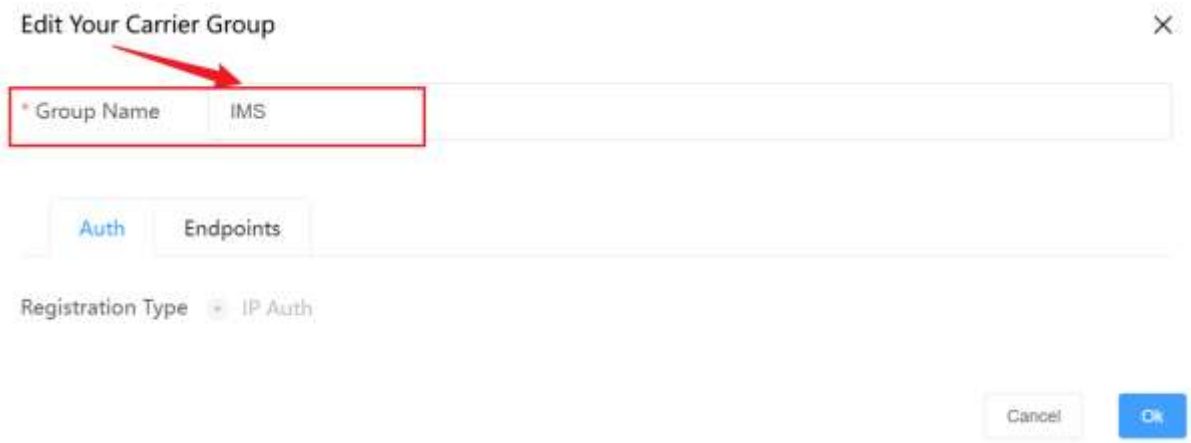


Figure13 Fill in the group name

Step.3 Click Endpoints > Add to add operator details.

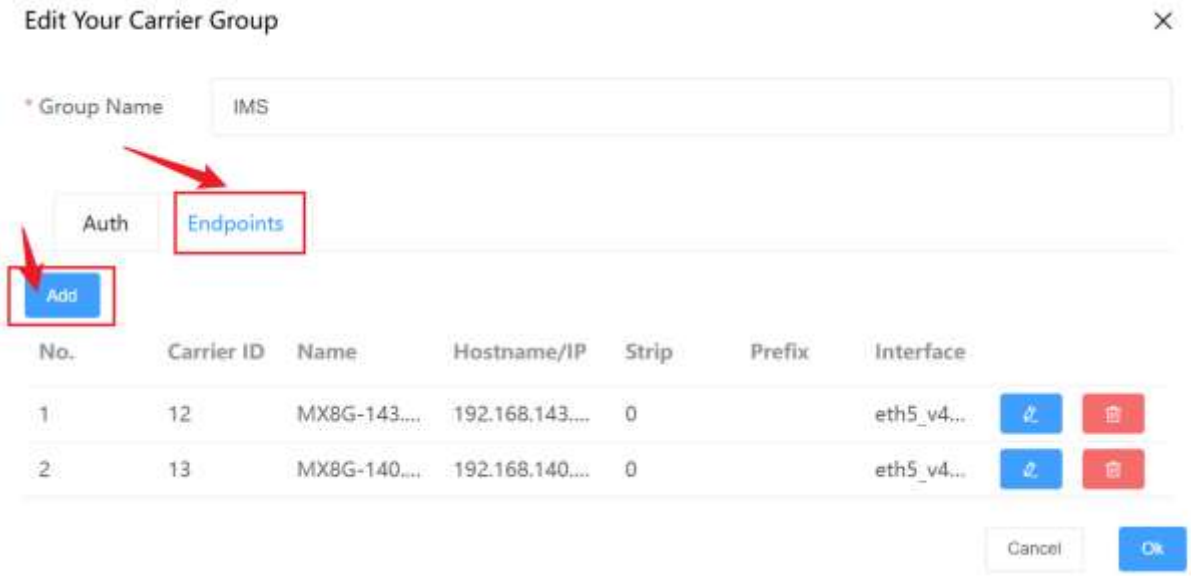


Figure14 Edit Operator Group

 Copyright © Redstone Systems, Inc

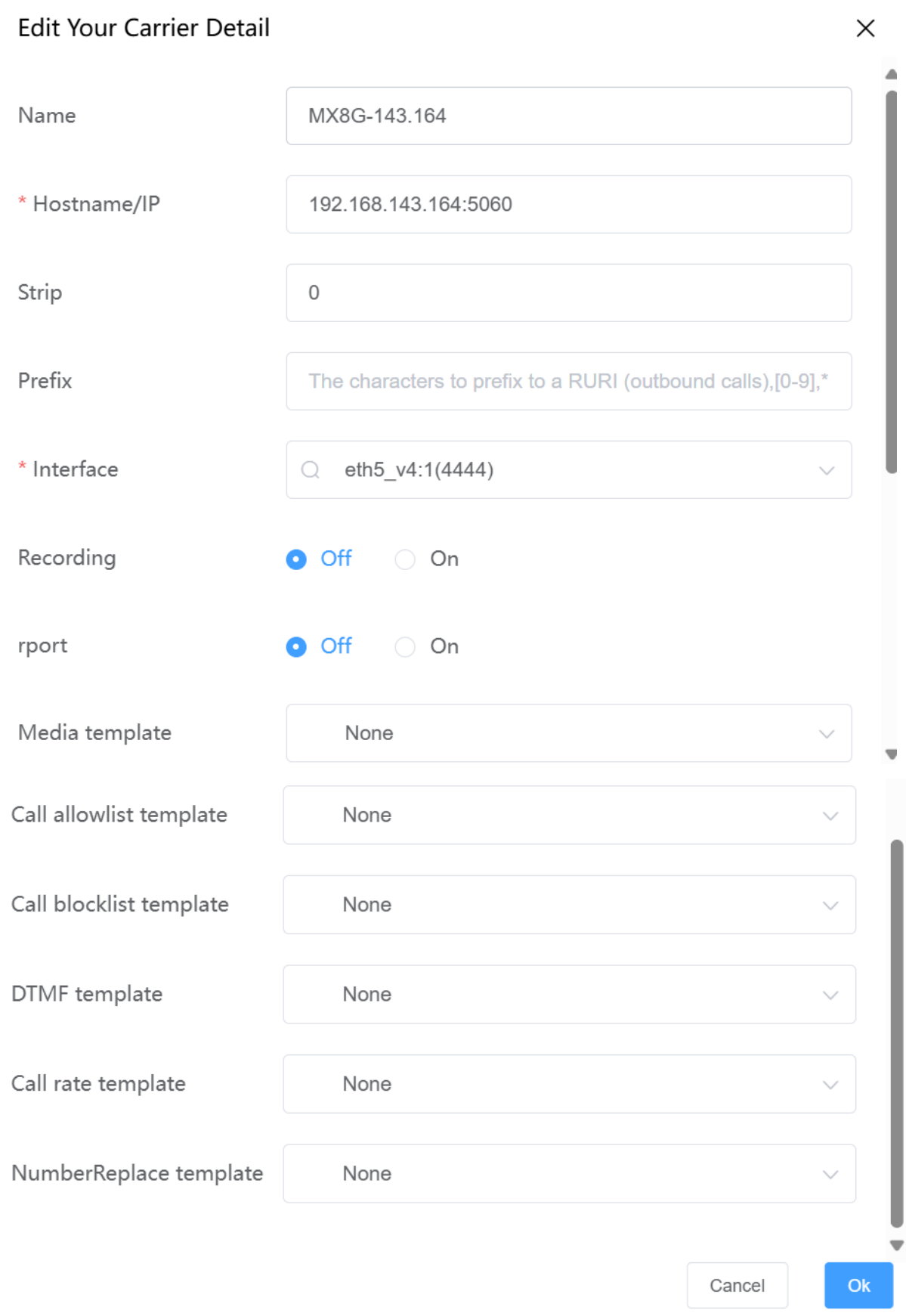


Figure15 Adding Operator Group Details

 Copyright © Redstone Systems, Inc

Table13 IP Certification

Item	Definition
Hostname/IP	The hostname or IP address of the operator, which is used to establish a network connection to the operator.
Hostname/ IP: port	The hostname or IP address of the operator followed by the port number. The port number defaults to 5060.
First digit removal	Number of characters to be removed from the RURI (outbound calls). A certain number of characters to be used to remove from the URI of a call request.
Add Prefix	Adds a prefix to the RURI of an outbound call. Prefixes can be a combination of digits [0-9], *, #, and + for modifying call numbers.
outgoing interface	Select the outbound interface to specify the network to which outbound calls flow.
sound recordings	Set the recording function to record the audio content of outbound calls when it is turned on and not when it is turned off.
Rport	Set whether to enable the Rport function.Rport is used to support NAT penetration and ensure that packets can reach the target device correctly.
Media Templates	Set up call-related media templates for defining rules for processing media streams such as audio and video.
Call whitelisting templates	Select a call whitelist template for managing allowed calls to ensure that legitimate calls are connected without incident.
Call Blacklist Template	Select the Call Blacklist template for blocking unallowed calls and preventing malicious calls from getting through.
DTMF templates	Select the DTMF template for configuring the processing rules for key tones (DTMF).
Call frequency templates	Select a call frequency template for limiting the frequency of

 Copyright © Redstone Systems, Inc

	calls to prevent malicious call behavior.
Number Transformation Templates	Select a number transformation template for formatting call numbers, such as removing area codes, adding prefixes, etc.

Delete Endpoints

Click Delete in the lower right corner to delete the endpoint.

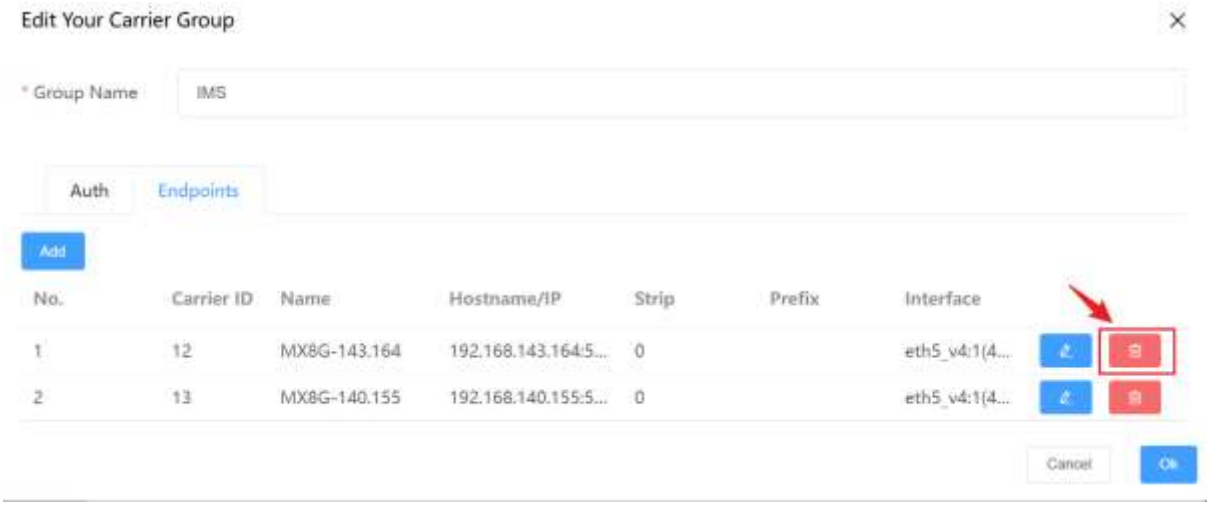


Figure16 Delete Endpoints

Refresh Node

Click Refresh to refresh the node information.



Figure17 Refresh Node

 Copyright © Redstone Systems, Inc

7.1.2 User Name/Password Authentication

Filtering Users

Enter the user name and authentication user name to quickly filter users.

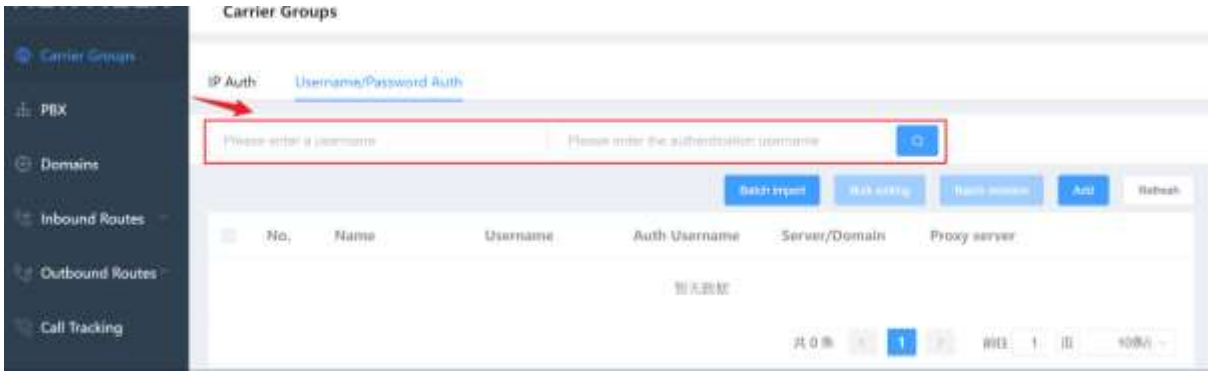


Figure18 Filtering Users

Batch Import

SBC supports batch import of operator groups.

Step.1 Select Outgoing Interface

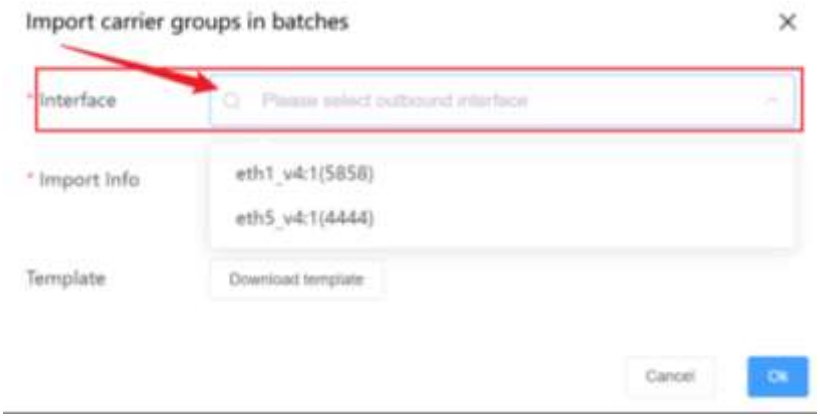


Figure19 Selecting an Outgoing Interface

Step.2 Importing information

 Copyright © Redstone Systems, Inc

Download Templates

Click Download Templates to download an import information template.



Figure20 Download Template

Batch Modify/Delete User Name Password Authentication

Click on the Bulk Modify/Delete button to perform bulk modification and deletion of user's username and password authentication.



Figure21 Bulk Modify/Delete Username Password Authentication

Add username/password authentication

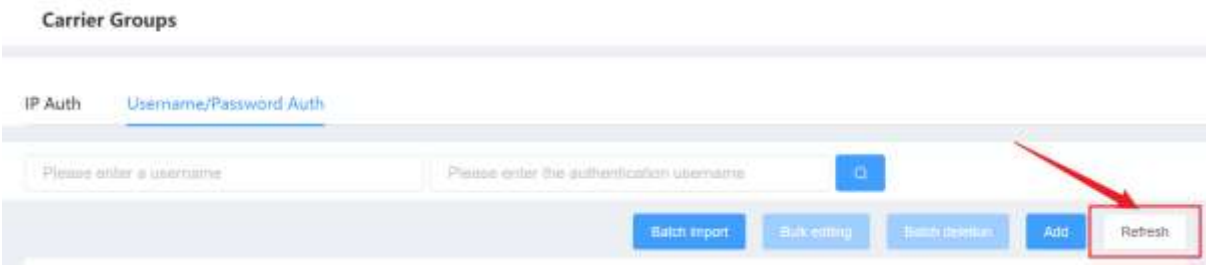
Table14 Add Username/Password Authentication

Item	Definition
user ID	Enter the registered user name provided by the operator for authentication in the system to ensure connection and authentication with the external registration server.
authentication code	Enter the password that accompanies the user name.
Authentication User Name	Enter the authentication username. Used to identify the

 Copyright © Redstone Systems, Inc

	account information that corresponds to the registered user name on the authentication server and is used to authenticate the source of the call request.
Registered Servers/Domains	Enter the registration server address or domain name provided by the operator for device or user registration. Ensure that the device can properly connect to the appropriate server.
proxy server	Enter the address or IP of the proxy server. The default setting of the proxy server's port is 5060, which is used to forward registration requests and manage network communication traffic.
outgoing interface	Select Outbound Interface is used to set up the communication interface for outbound calls to ensure that call requests can be outbound through the correct network path.

Refresh current username/password



 Copyright © Redstone Systems, Inc

7.2 PBX

Screening PBX

Enter a name/username to filter PBX devices.

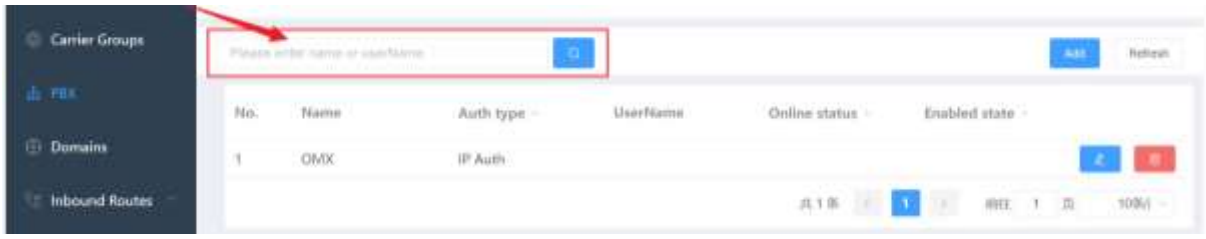


Figure22 Filtering the PBX

Add PBX details

Navigate to PBX and click Add to add PBX details.

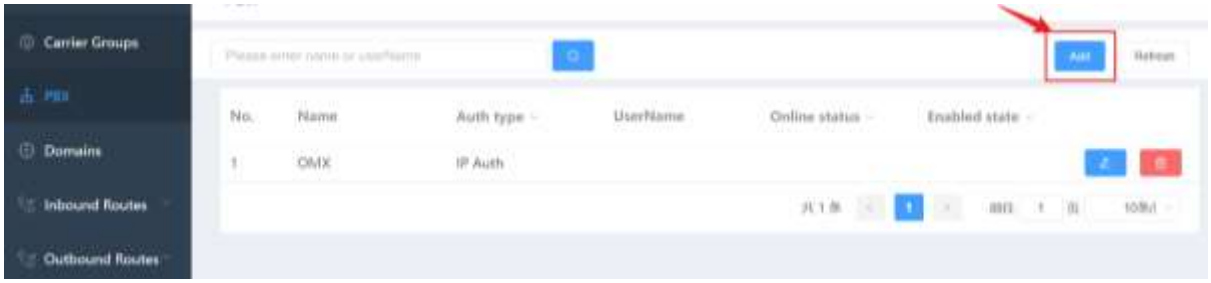


Figure23 Add PBX Details



Figure24 Add PBX Details 2

 Copyright © Redstone Systems, Inc

Table15 New PBX

Item	Definition
Item	The name of the PBX.
Maximum concurrent calls	Sets the maximum number of concurrent calls allowed by this PBX system. This value limits the maximum number of calls that can be processed at one time.
accreditation	Supports IP authentication and user name/password authentication.

Add Endpoints

Click Add in the lower left corner to add a new endpoint.



Figure25 New Endpoints

Table16 New Endpoints

Item	Definition
Hostname/IP	The hostname or IP address of the operator, which is used to establish a network connection to the operator.
Hostname/IP:port	The hostname or IP address of the operator followed by the port number. The port number defaults to 5060.
First digit removal	Number of characters to remove from the RURI (outbound calls). A certain number of characters to be removed from the

 Copyright © Redstone Systems, Inc

	URI for call requests.
Add Prefix	Adds a prefix to the RURI of an outbound call. Prefixes can be a combination of digits [0-9], *, #, and + for modifying call numbers.
outgoing interface	Select the outbound interface to specify the network to which outbound calls flow.
sound recordings	Set the recording function to record the audio content of outbound calls when it is turned on and not when it is turned off.
Rport	Set whether to enable the Rport function. Rport is used to support NAT penetration and ensure that packets can reach the target device correctly.
Media Templates	Set up call-related media templates for defining rules for processing media streams such as audio and video.
Call whitelisting templates	Select a call whitelist template for managing allowed calls to ensure that legitimate calls are connected without incident.
Call Blacklist Template	Select a call blacklist template for blocking unallowed calls and preventing malicious calls from getting through.
DTMF templates	Select the DTMF template for configuring the processing rules for key tones (DTMF).
Call frequency templates	Select a call frequency template for limiting the frequency of calls to prevent malicious call behavior.
Number Transformation Templates	Select a number transformation template for formatting call numbers, such as removing area codes, adding prefixes, etc.

 Copyright © Redstone Systems, Inc

Refresh List

Click the Refresh button on the right to refresh the list.



Figure26 refreshes the list

Filter List by Type

Click on the list's option box to filter by type.

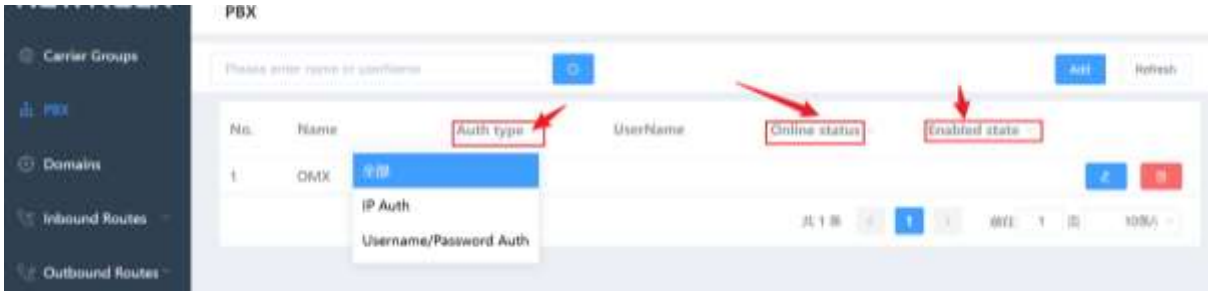


Figure27 Filter list by type

Edit/Delete Endpoint Information

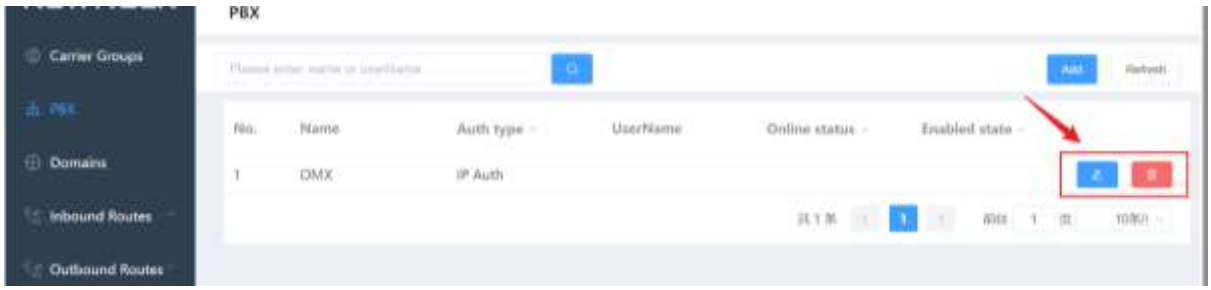


Figure28 Edit/Delete Endpoint Information

7.3 Domain Management

New Domain

Step .1 Navigate to Domain Management, click Add, and fill in the relevant configuration information.



Figure29 New Domain

Table17 New field

Item	Definition
domain name	Enter the domain names to be added, for example: domainA.com, domainB.com. Multiple domain names can be separated by commas.
Domain type	Please select the type of this domain by choosing the appropriate domain type from the drop down menu. (Forward Registrations and Calls/Forward Calls Only Calls)
mapping endpoint	Enter a PBX ID that will be mapped to the domain. This field points to the identifier of the PBX.
note	Provide a description or note about the domain.

Screening Domain

Entering a domain name says that the domain can be filtered.

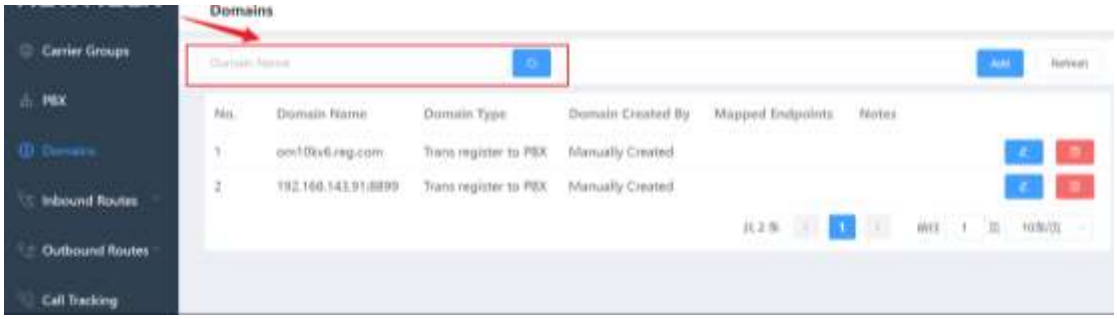


Figure30 Filter Fields

 Copyright © Redstone Systems, Inc

7.4 Inbound Signaling (Computing)

7.4.1 Number Routing

Navigate to Inbound Routing > Number Routing and click Add to add a new number route.

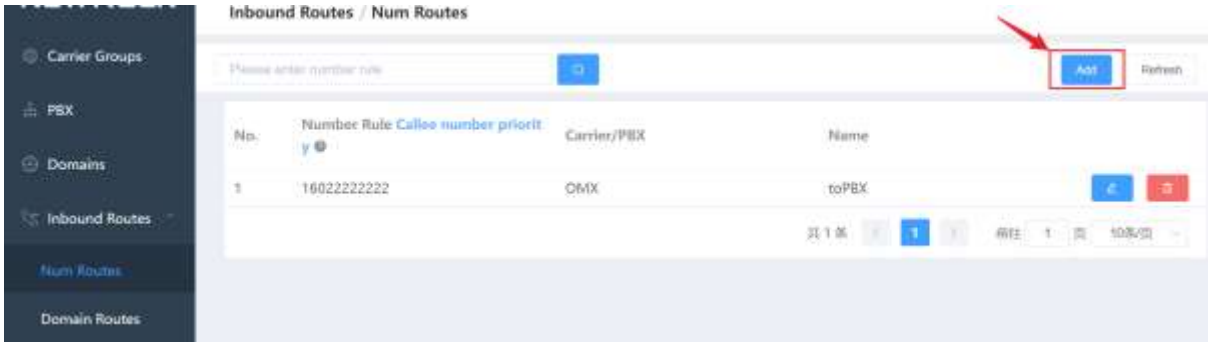


Figure31 number routing

Table18 Number Routing

Item	Definition
Item	Enter a name for this inbound mapping rule that identifies the rule.
Numbering Rules	Input number rules, for example: 136XXXXX:X means any number 0-9 1 digit, +123[0-2,3][0-9]:0 is used to match a specific pattern. Regular expressions are used here to Definition the matching rules, and the supported characters include: [0-9]: match any number from 0 to 9. [a-zA-Z]: match any letter. [1,2,3]: match any one of 1, 2 or 3.
Called Number Conversion	Sets the target number for called number conversion that the rule matches to.
Carrier/PBX	Select the carrier or PBX (IMS, OMX, OMX LB) to which the rule applies. Select the appropriate carrier or PBX for this inbound call as needed.
failover forwarding	Set whether to enable failover forwarding to ensure calls can be received by other rules or targets. Support for called number translation and carrier/PBX (IMS, OMX, OMX LB)

 Copyright © Redstone Systems, Inc

7.4.2 Domain Name Routing

Click New to add a new domain route.



Figure32 Domain Name Routing

Table19 Domain Name Routing

Item	Definition
Item	Enter a name for this domain name route that identifies the route.
domain name of the primary caller (i.e. the name of the domain that is to be called)	Enter the domain name of the calling party to indicate which calling domain name this route applies to. Note: Route prioritization rules can be modified in 'Application Configuration'.
Carrier/PBX	Select the carrier or PBX system type that applies to this route. (IMS, OMX, OMX LB)

7.5 Routing (For Callsign)

7.5.1 Number Routing

Navigate to Outbound Routing > Number Routing and click Add to configure outbound routing.

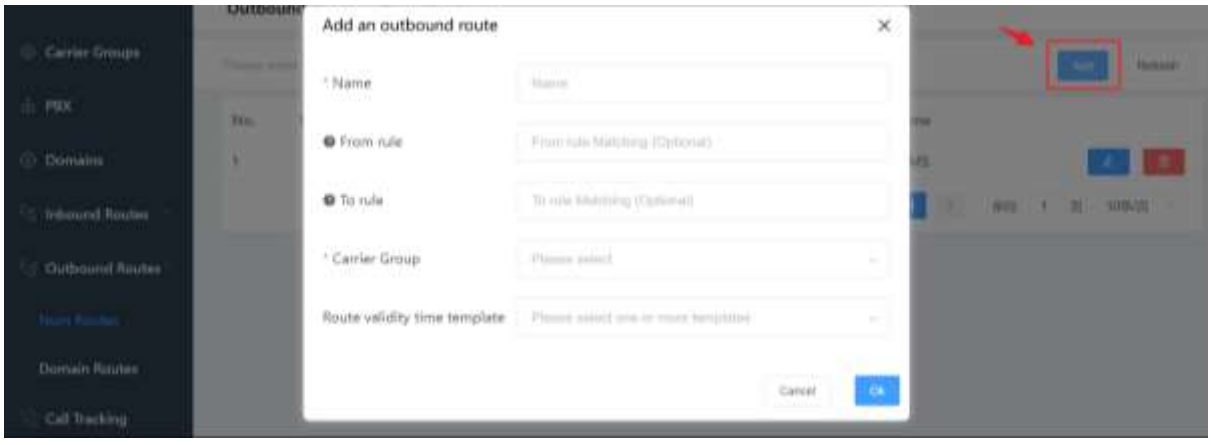


Figure33 Number Routing

 Copyright © Redstone Systems, Inc

Table20 Number Routing

Item	Definition
Item	Enter the name of this outgoing route, which is used to identify and differentiate between different routes.
Calling rules	Enter the rules for the calling number.
The called rules	Enter the rule for the called number.
operator group	Select the carrier group to which this route applies.
Routing Effective Time Template	Select one or more time templates for the routing to take effect.

Edit/Delete

Click Edit/Delete in the lower right corner to delete the corresponding item.

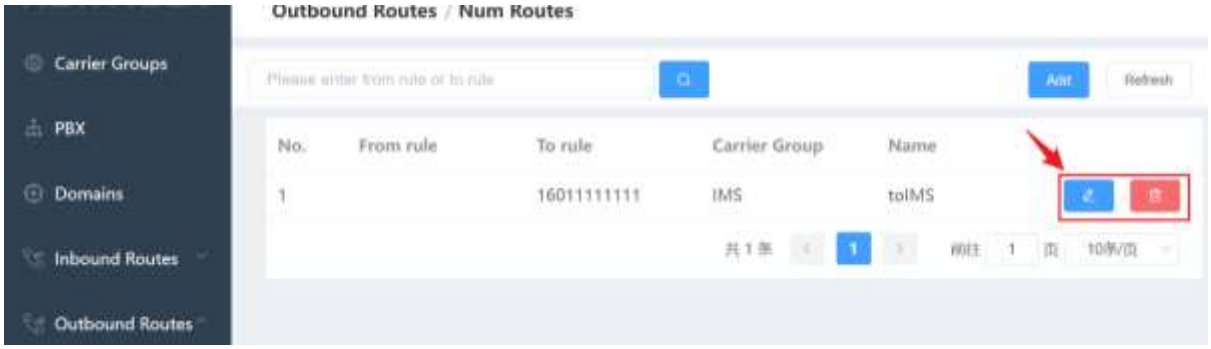


Figure34 Edit/Delete

7.5.2 Domain Name Routing

Click Add in the lower left corner to add domain routing.

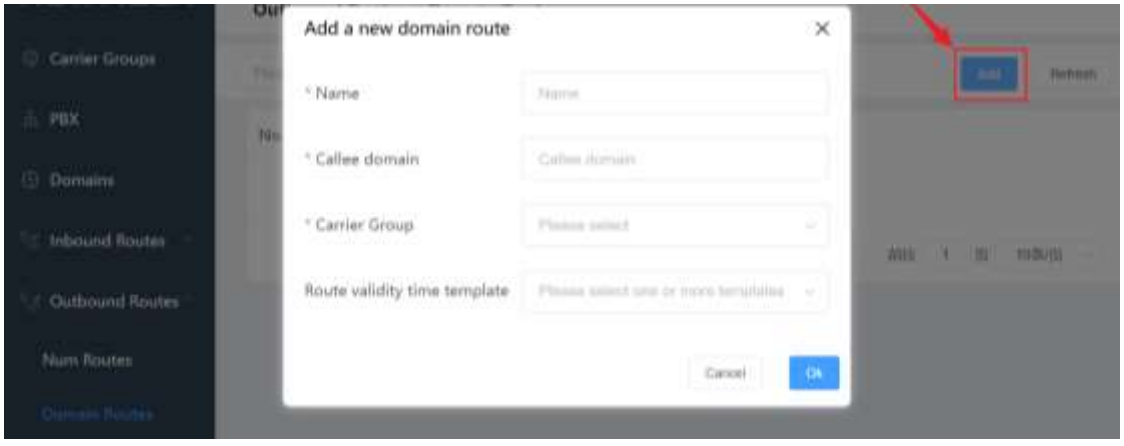


Figure35 Adding a Domain Route

 Copyright © Redstone Systems, Inc

Table21 Add Domain Routing

Item	Definition
Item	Enter the name of this outgoing route, which is used to identify and differentiate between different routes.
Calling rules	Enter the rules for the calling number.
The called rules	Enter the rule for the called number.
operator group	Select the carrier group to which this route applies.
Routing Effective Time Template	Select one or more time templates for the routing to take effect.

7.6 Call Tracking

Navigate to Call Tracking and click New to add a call tracking configuration.

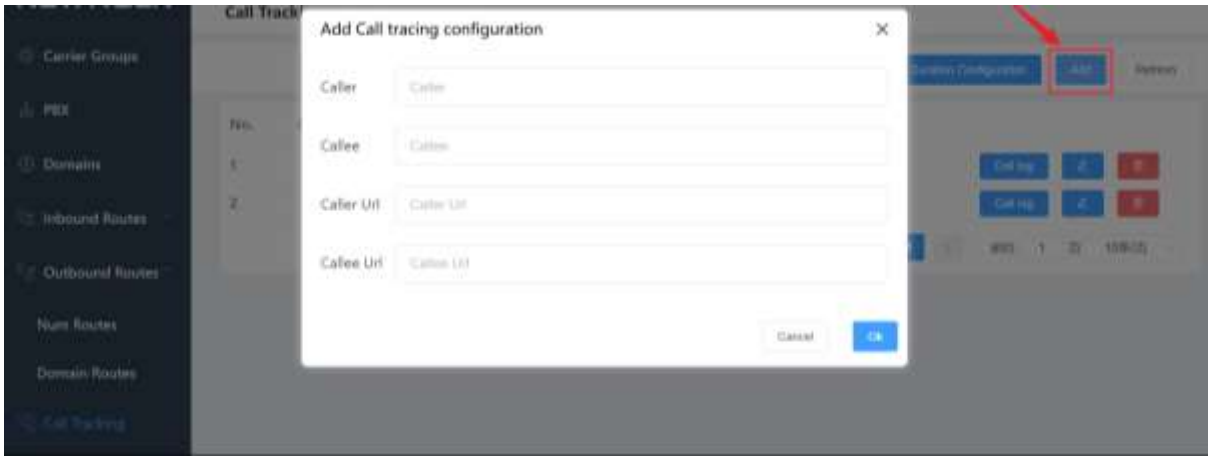


Figure36 Call Tracking

Table22 Call Tracking

Item	Definition
caller	Enter or select information about the calling party to specify the party initiating the call.
called	Enter or select information about the called party that is used to specify the party that will answer the call.
calling address	Enter the IP address or domain name of the calling party.
called address	Enter the IP address or domain name of the called party.

 Copyright © Redstone Systems, Inc

Retained time-configuration

Click Retention Time Configuration to set the retention time as desired.

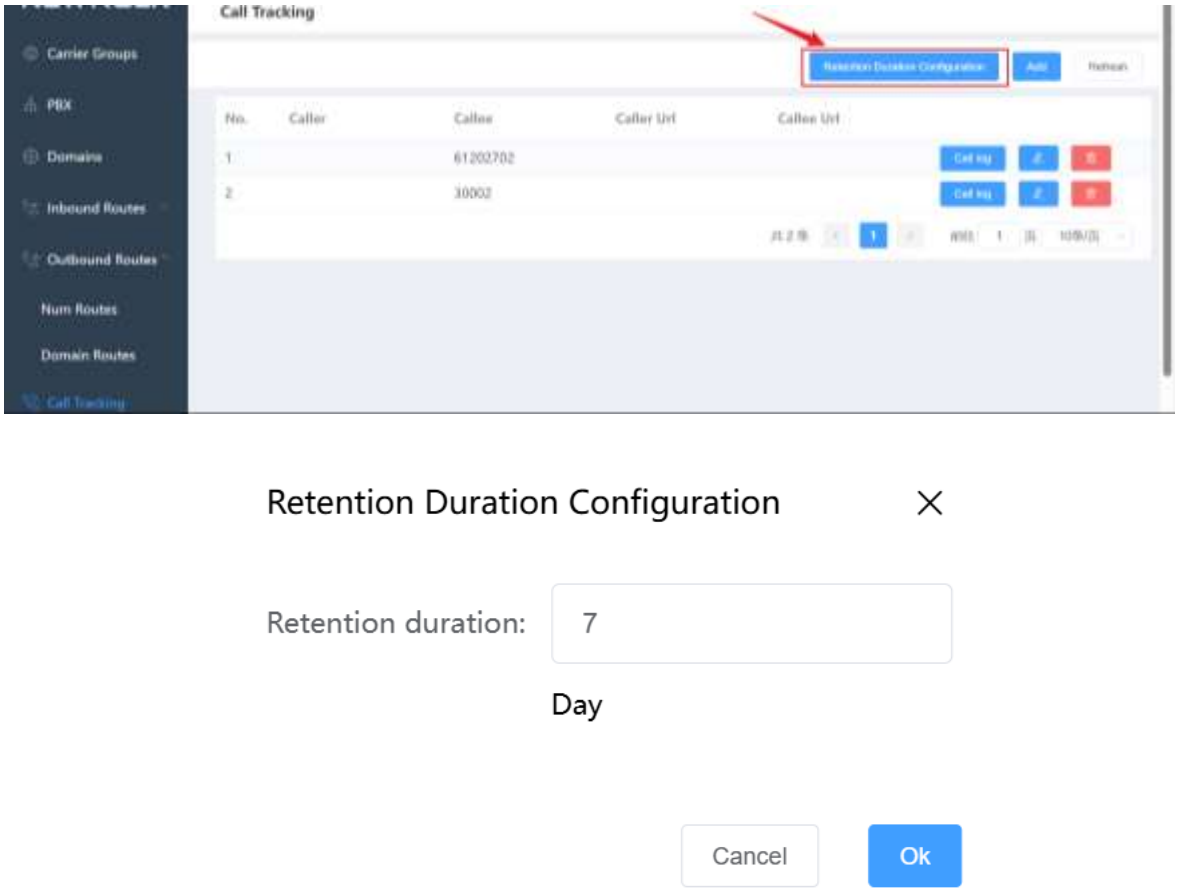


Figure37 Reserved Timing Configuration

7.7 Network Management

7.7.1 Network Setup

Default Route Configuration

Navigate to Network Management > Network Configuration to edit the network configuration for the corresponding interface.

 Copyright © Redstone Systems, Inc



Figure38 Network Settings

Table23 Network Settings

Item	Definition
interface name	Select or enter the name of a network interface through which data traffic is sent. The interface name is usually associated with a physical or virtual network interface in the system.
default gateway	Enter the IP address of the default gateway. The default gateway is the address of the router or network device through which packets are forwarded to other networks when there is no clear destination.

network setup

Navigate to Network Management > Network Settings to allow administrators to configure the device's network interface, including parameters such as static IP address, subnet mask, DNS server, and static routing.

 Copyright © Redstone Systems, Inc

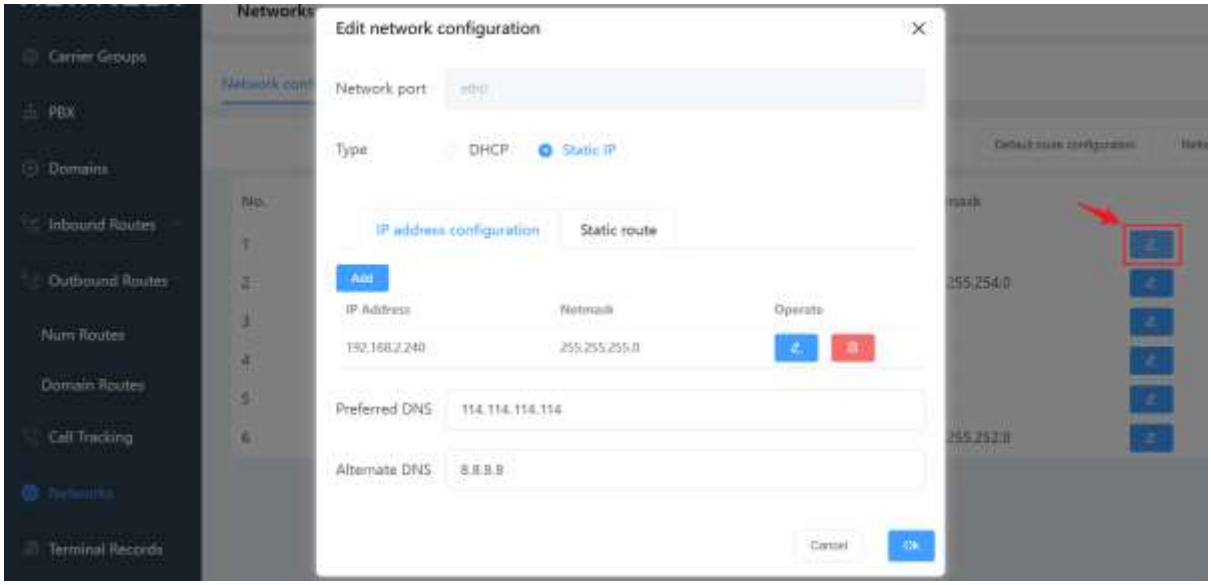


Figure39 Network Setup 2

Table24 Network Settings

Item	Definition
Port Name	Sets the name of the network interface to identify the network interface.
typology	Select the type of network interface, you can choose "DHCP" and "Static IP" type.
Preferred DNS	Configure the IP address of the preferred DNS server, which is used to resolve domain names to IP addresses.
Alternate DNS	Configure the IP address of the backup DNS server for backup resolution when the preferred DNS is not available.

 Copyright © Redstone Systems, Inc

7.7.2 Port Configuration

New listening port

Navigate to Network Management > Port Configuration and click Add Listening Port.



Figure40 New listening port

Table25 Port Configuration

Item	Definition
ports	Configure the port number to listen on.
Port Name	Select the name of the network port on which the port is listening.
pact	Select the network protocol to listen to. Supported protocols: UDP, TCP, TLS.
NAT address	Configure the address used during Network Address Translation (NAT) for mapping network addresses between the intranet and extranet.

 Copyright © Redstone Systems, Inc

global configuration

Table26 Global Configuration

Item	Definition
NAT Pings Interval	Configure the time interval in seconds for NAT Pings to be sent. This item is used to send ping requests to remote terminals periodically to prevent NAT form timeout. 0 means disable this function and no ping request will be sent, Range: 1 - 600 seconds.
NAT Pings package	This field configures the destination for sending ping packets. In general, the system periodically sends ping packets to the IP addresses of registered endpoints to keep the session active and prevent connection disconnection due to NAT routing timeout.

Encryption Algorithm

Click Edit Listening Port Configuration to set the encryption algorithm and key.

Table27 Encryption Algorithm

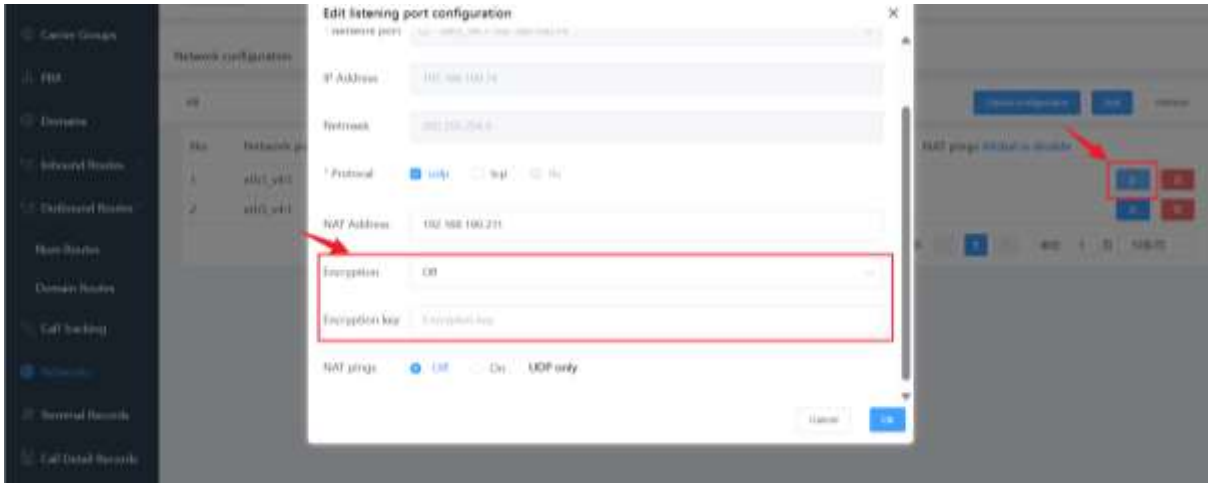


Figure41 encryption algorithm

 Copyright © Redstone Systems, Inc

7.8 Terminal Records

Displays the registration information, contact information, and source address information related to each terminal device in the terminal record screen. Quick filtering is supported.



Figure42 Terminal Records

7.9 Call Record

Navigate to > Call History, which supports filtering, playing, downloading and deleting historical call history.

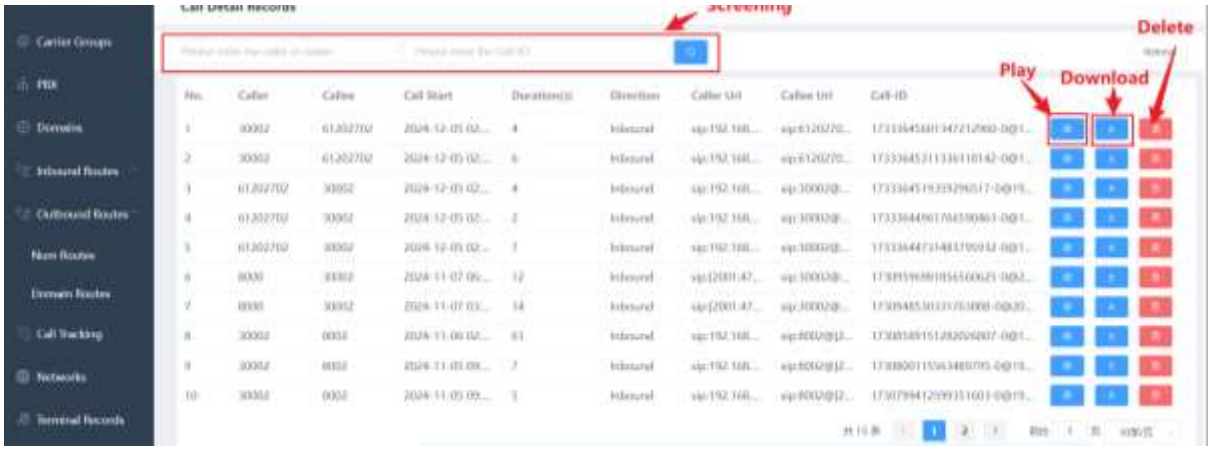


Figure43 Call Log

Table28 Call Log

Item	Definition
caller	The user name or number of the user or terminal that initiated the call.
called	The user name or number of the user or terminal receiving the call.
Starting time	The timestamp of the start of the call.
Duration (seconds)	The duration of the call in seconds.
calling mode	Inbound/outbound.
calling address	The address of the party initiating the call.

 Copyright © Redstone Systems, Inc

called address	The address of the receiving caller.
Call-ID	A unique identifier for each call that identifies a call session.

7.10 Template Management

7.10.1 Call black and white list templates

Navigate to Template Management > Call Black and White List for flexible configuration of black and white list called number prefix rules.

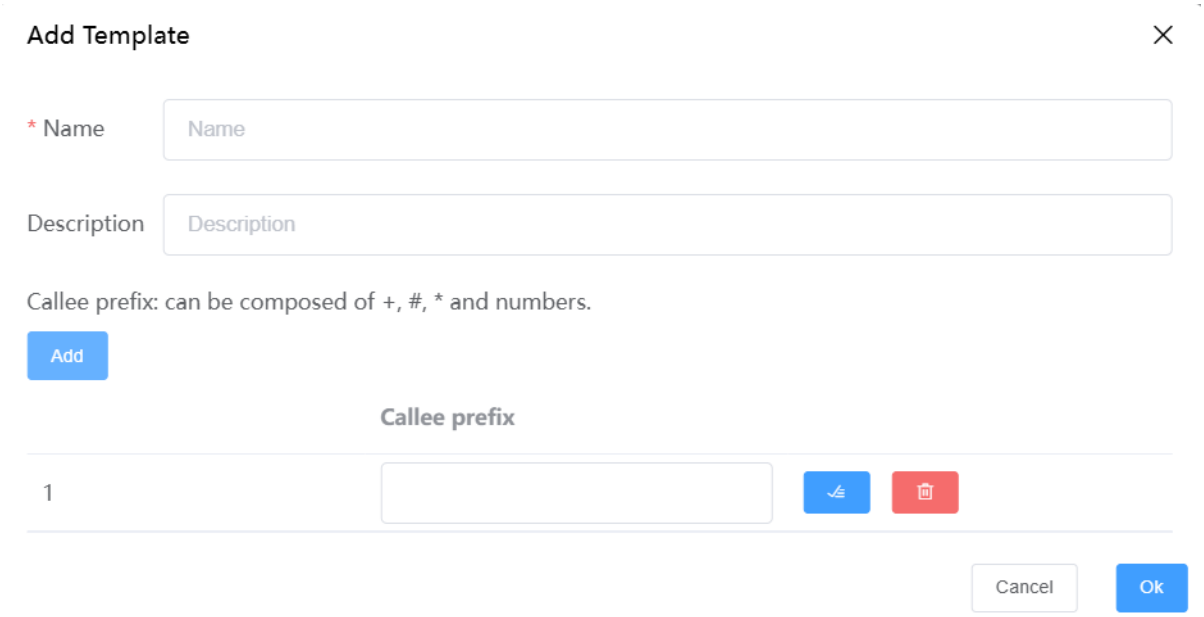


Figure44 New Template

Table29 New Template

Item	Definition
Item	The name configured to identify this called number prefix rule.
descriptive	A detailed description of this configuration.
prefix of the called number	A prefix rule used to specify the called number. The prefix can consist of characters such as numbers, symbols (e.g., +, #, *), etc.

 Copyright © Redstone Systems, Inc

7.10.2 DTMF Templates

Navigating to Template Management > DTMF, the administrator can create and manage transmission templates for DTMF (Dual Tone Multi-Frequency) signals.



Figure45 New DTMF template

Table30 New DTMF template

Item	Definition
Item	Configure the name of the template to identify and differentiate between different DTMF templates.
descriptive	A description of the template.
transmission method	Selects the transmission method for this DTMF template. RFC2833, SIP INFO and Transmission are supported.

 Copyright © Redstone Systems, Inc

7.10.3 Call Frequency Templates

Navigate to Template Management > Call Frequency Templates. On the New Call Frequency Template Configuration screen, administrators can Definition parameters such as Call Frequency per Second and Maximum Concurrent Calls, which are used to control and manage the load and resource usage of the calling system.



Figure46 Call Frequency Template

Table31 Call Frequency Template

Item	Definition
Item	Configure the name of the template to identify and differentiate between different call frequency templates.
descriptive	A description of the template to help administrators understand the specific application and configuration purpose of the template.
call rate	Sets the maximum number of calls per second, if set to 0, it means no call rate limitation.
Maximum number of concurrent calls	Sets the maximum number of concurrent calls; if set to 0, it means that the number of concurrent calls is not limited.

 Copyright © Redstone Systems, Inc

7.10.4 Media Codec Templates

The configuration screen of the New Media Codec Template allows administrators to Definition the codecs to be used during media transmission. This configuration is primarily used to select and manage the codecs (Codecs) supported in voice calls, thus ensuring the quality and compatibility of voice communications.



Figure47 Media Codec Template

Table32 Media Codec Template

Item	Descriptive
Item	Configure the name of the template to identify and differentiate between different media codec templates.
descriptive	A description of the template.
codecs	Select the type of codec supported by this template.
Enabled codes	Select the enabled codec method.
Disabled codes	Select the disabled codec.

 Copyright © Redstone Systems, Inc

7.10.5 Routing Effective Time Template

Navigate to > Template Management > Routing Effective Time, where the Time Rule Template Configuration screen allows administrators to set specific time period rules for business processes, call routing, or other features that require time-based restrictions.

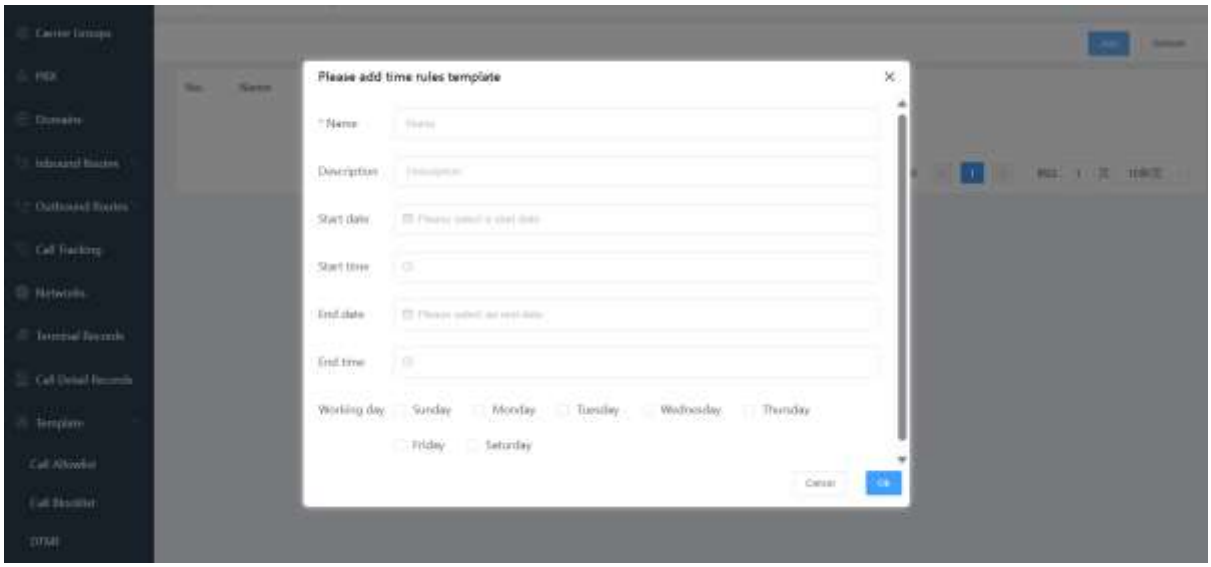


Figure48 Routing Effective Time Template

Table33 Routing Effective Time Template

Item	Definition
Item	The name of the template that identifies and distinguishes the different time rule templates.
descriptive	A description of this time rule template.
Start date	The start date of the rule's entry into force .
Starting time	The start time for the rule to go into effect.
End date	The date on which the rule ends.
end time	Time for the rule to end.
workdays	Select the applicable weekday to set the day of the week to take effect.

 Copyright © Redstone Systems, Inc

7.10.6 Number Change Template

Navigate to Template Management > Number Changes to configure the rules for replacing the calling and called numbers.



Figure49 Number Change Template

Table34 Change of Number Template

Item	Definition
Item	The name of the template that identifies and distinguishes the different number replacement rule templates.
descriptive	A description of the number replacement rule template.
Calling Number Replacement Rules	Setting the replacement rules for the calling number, supporting a variety of rule Formats
Called Number Replacement Rules	Setting the replacement rules for called numbers, supporting various rule Formats

 Copyright © Redstone Systems, Inc

7.11 Application Configuration

7.11.1 SIP Configuration

Navigate to Application Configuration > SIP Configuration, the configuration interface is used to adjust network latency management and data transmission optimization in SIP communication, as well as to support customizing SIP header fields and configuring SIP request/response message formats.

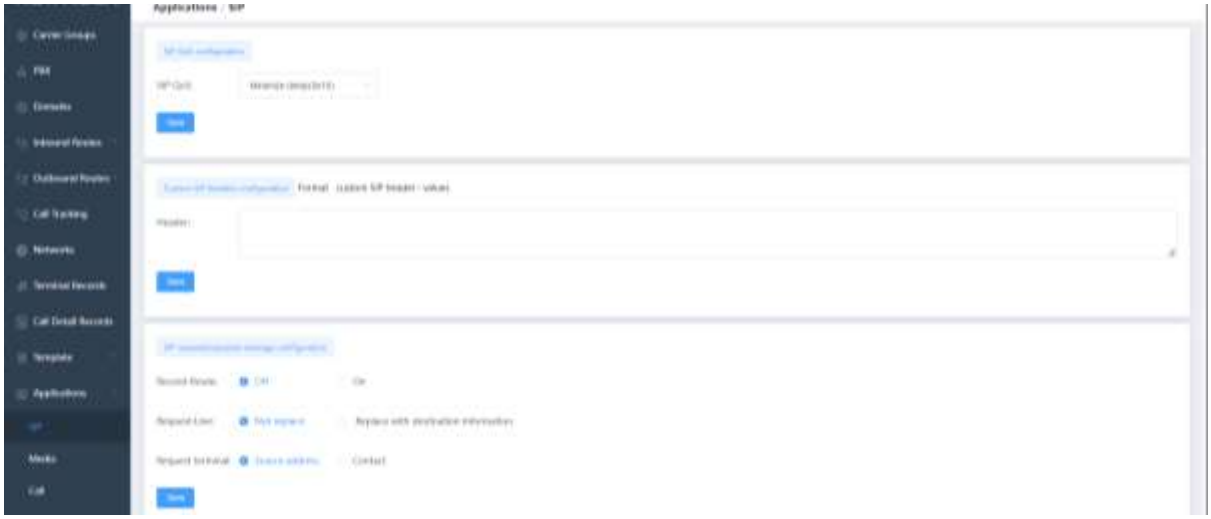


Figure50 SIP Configuration

Table35 SIP Configuration

Item	Definition
SIP QoS	Used to configure Quality of Service settings for SIP communications, supporting Minimize Latency (0x10), Maximize Throughput (0x08), Maximize Reliability (0x04) and Minimize Cost (0x02).
SIP header field configuration Fromat	Set up customized SIP header fields. Users can manually enter SIP header fields and their corresponding values.
SIP request/response message configuration	Configure specific fields in SIP request and response messages to optimize message routing and end-to-end information transfer.
Record-Route	Enables or disables the Record-Route header field, which is used to record route information.

 Copyright © Redstone Systems, Inc

Request-Line	Configure the request line, optionally without replacing it/replacing it with information about the destination.
Request terminal	Sets the type of requesting endpoint, with optional substitutions for source address and port or Contact address.

7.11.2 Media Configuration

Navigate to Application Configuration > Media Configuration. The Media Configuration interface is mainly used to optimize the quality of RTP data streams and port configuration, and also handles the configuration of media addresses and NAT-related settings.



Figure51 Media Configuration

Table36 Media Configuration

Item	Definition
RTP QoS	Configure RTP quality of service (QoS) parameters to optimize the transmission of RTP media streams.
RTP Port Min.	Sets the minimum value for the RTP port. The range is 10000 to 65535.
RTP Port Maximum	Sets the maximum value of the RTP port. The range is 10000 to 65535.
Media Address	Configure the media address, set the local address as well as the NAT address.
Media Address Self-Learning	Enable or disable the media address self-learning feature.

 Copyright © Redstone Systems, Inc

7.11.3 Call Configuration

Navigate to Application Configuration > Call Configuration, in this configuration interface, the administrator can set various parameters related to calls, including the selection of the IP trunk mode, the priority configuration of routing rules, the maximum length of the PBX username, and the interval of sending OPTIONS messages for PBX endpoints.



Figure52 Call Configuration

Table37 Call Configuration

Item	Definition
IP Relay Mode	Configure the working mode of IP trunk, you can choose redundant mode or load balancing mode. Redundancy mode is used to ensure automatic switching to the backup line when the primary line fails; load balancing mode is used to balance the call traffic and improve the overall system throughput. IP Relay Redundancy Mode: Enable the redundancy mode, when the main IP relay fails, it will automatically switch to the backup line to ensure the communication is not interrupted. IP Trunking Load Balancing Mode: Enable

 Copyright © Redstone Systems, Inc

	Load Balancing Mode to distribute call loads to multiple trunks to enhance the system's processing power and performance.
Inbound Routing Configuration	Configure routing rules for incoming calls, including number matching rules, routing priority, etc., to ensure that incoming calls are accurately routed to the correct destination. Number Matching Rule: Set up the matching rule for incoming call number, match and select route according to the incoming call number to ensure the incoming call can be correctly routed to the target endpoint. Supports matching only the called, only the caller, priority of called number, priority of caller number. Route Priority Rule: Set the route priority for incoming calls, you can choose "Called Number Priority", "Number Route Priority" or "Domain Name Route Priority" to control the route selection Route Priority: Set the route priority for incoming calls.
Outbound Routing Configuration	Configure the routing priority for outgoing calls to ensure that calls are able to select the most appropriate routing path, improving the quality and efficiency of calls. Route Priority Rule: Set the route priority for incoming calls, you can select "Called Number Priority", "Number Route Priority" or "Domain Route Priority" to control the route selection Route Priority: Set the route priority for incoming calls.
PBX username maximum length configuration	Configure the maximum length of the user name in the PBX system to ensure that the user name is entered in accordance with the system's length requirements. This option supports customized configuration.

 Copyright © Redstone Systems, Inc

PBX Endpoint Configuration	Sets the interval at which OPTIONS messages are sent to detect the status and availability of the endpoint.

7.11.4 Call Black/White List

Navigate to Application Configuration > Call Black/White List for flexible configuration of call black/white lists. Calls are prioritized to detect the configured global black/white list before detecting the black/white list in the template.



Figure53 Call Black/White List

Table38 Call Black/White List

Item	Definition
Item	The name configured to identify this called number prefix rule.
descriptive	A detailed description of this configuration.
prefix of the called number	A prefix rule used to specify the called number. The prefix can consist of characters such as numbers, symbols (e.g., +, #, *), etc.

 Copyright © Redstone Systems, Inc

7.12 Security Management

7.12.1 WEB Defense

Navigate to Security Management > WEB DEFENSE. In the Web Defense configuration interface, administrators can set up security measures for web applications, especially to prevent malicious attacks (such as brute-force cracking, DDoS attacks, etc.) from affecting the system.



Figure54 WEB DEFENSE

Table39 WEB DEFENSE

Item	Definition
Web defense	Enables or disables Web Defense, which is used to protect Web applications from external attacks.
time interval	Set the time interval for defense rules.
Retries	Sets the maximum number of attempts allowed in a given time interval.
sanitization	Sets the amount of time a user is banned from access when the retry count is reached. Prevents malicious attackers from bypassing restrictions by making frequent attempts.

 Copyright © Redstone Systems, Inc

7.12.2 SSH Defense

Navigate to Security Management > SSH Defense, and in the SSH Defense configuration interface, administrators can set the security protection policy for SSH services. This configuration is used to prevent malicious attackers from accessing the server by means such as brute-force breaking.

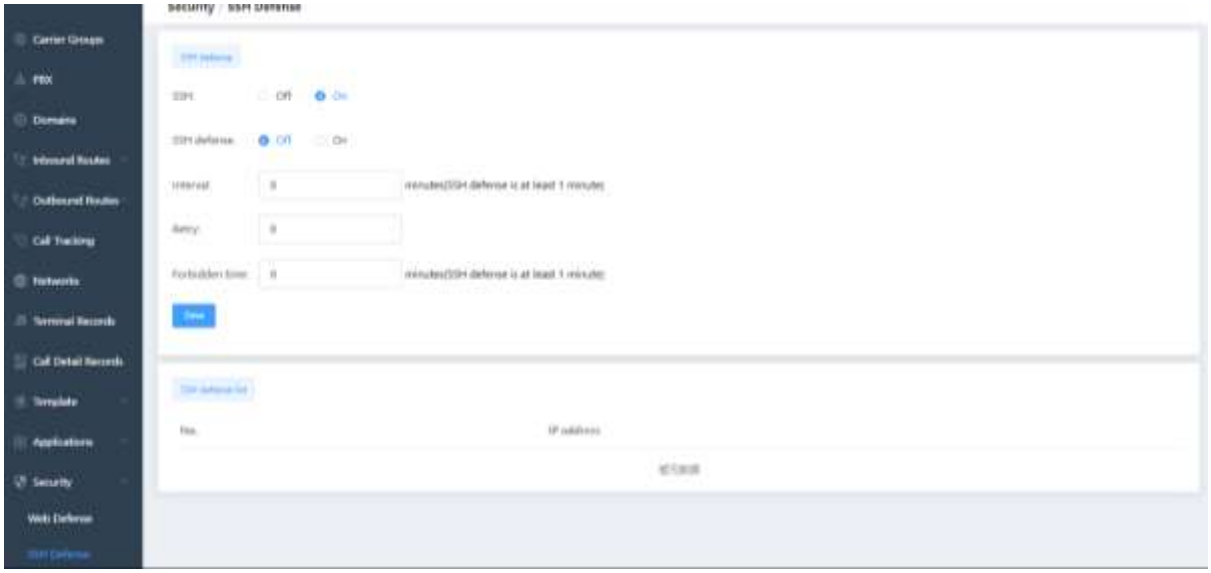


Figure55 SSH Defense

Table40 SSH Defense

Item	Definition
SSH defense	Enable or disable SSH defense to prevent malicious attacks via SSH protocol.
time interval	Sets the time interval for defense rules, indicating the minimum time interval between two SSH login attempts.
Retries	Set the maximum number of attempts allowed in the specified time interval. After this number of attempts is exceeded, the system performs defensive measures (e.g., prohibiting SSH login).
sanitization	Set the length of time to disable login after the number of retries is reached to prevent attackers from bypassing the limit by making frequent attempts.

 Copyright © Redstone Systems, Inc

7.12.3 SIP Defense

Navigate to Security Management > SIP Defense. In the SIP Defense configuration interface, administrators can set up protection mechanisms against the SIP protocol to prevent SIP services from being attacked, especially against DDoS attacks, brute force decryption, and abusive behavior.



Figure56 SIP Defense

Table41 SIP Defense

Item	Definition
SIP Defense	Enable or disable the SIP protocol defense function to prevent the SIP protocol from being maliciously attacked or abused.
time interval	Sets the time interval of the defense rule, indicating the maximum number of SIP packets allowed in this time interval.
Maximum number of packets	Set the maximum number of SIP requests allowed in the time interval, beyond which the system will trigger defense measures.
sanitization	Set the time to disable SIP traffic after the maximum number of packets is reached to prevent malicious attacks from continuing.

 Copyright © Redstone Systems, Inc

7.12.4 Other Defenses

Navigating to Security Management > Other Defenses, administrators can configure defense mechanisms for different types of attacks, including Ping Attack Defense, UDP-Flood Attack Defense, and TCP-Flood Attack Defense.



Figure57 Other defenses

Table42 Other Defense

Item	Definition
anti-ping	Controls whether defense against Ping requests (ICMP requests) is enabled. Prevents Ping Flood attacks or malicious Ping requests.
UDP-Flood Attack Defense	Configure whether to enable the UDP Flood attack defense mechanism to prevent large-scale UDP packet attacks that consume bandwidth or cause service interruptions.

7.12.5 Access to black and white lists

Navigate to Security > Access Black & White List, where the administrator can set the IP addresses that are allowed or prohibited from accessing the system web interface.



Figure58 Accessing the Black and White List

 Copyright © Redstone Systems, Inc

Table43 Access to Black and White Lists

Item	Definition
whitelisting	Configure the list of IP addresses that are allowed to access the web interface, only IP addresses in this list can access the web interface.
blacklists	Configure a list of IP addresses that are prohibited from accessing the Web interface; the listed IP addresses will not be able to access the Web interface

7.13 System Management

7.13.1 System Configuration

Navigate to System Management>System Configuration, in the License Authorization Management interface of the system, administrators can view and manage the system's license information, including the certificate application code, the maximum number of concurrency, and the number of manageable terminals. To purchase a license, please contact your distributor.



Figure59 System Configuration

7.13.2 Log Management

Navigate to System Management > Log Management. In the Log Management interface, administrators can configure and view all kinds of log information of the system.



Figure60 Log Management

 Copyright © Redstone Systems, Inc

Table44 Log Levels

Item	Definition
Log level	Controls the level of logging detail, there are usually different levels, such as debug, info, warn, error, when set to debug, the most detailed log information will be recorded.
Call debugging	Enables or disables call-related debug logging, which is typically used to debug call-related features. When enabled, you can view the processing of each call in detail.
Current log downloads	Provides the function of downloading the current system log, administrators can download the log file locally for further analysis or backup.
Log migration	This function is used to move log files from the current storage directory to other storage locations for freeing up storage space.

Historical System Log/Call Log

The system supports viewing historical system logs and call logs, and the download button in the lower right corner of the stand-alone machine can be downloaded immediately.

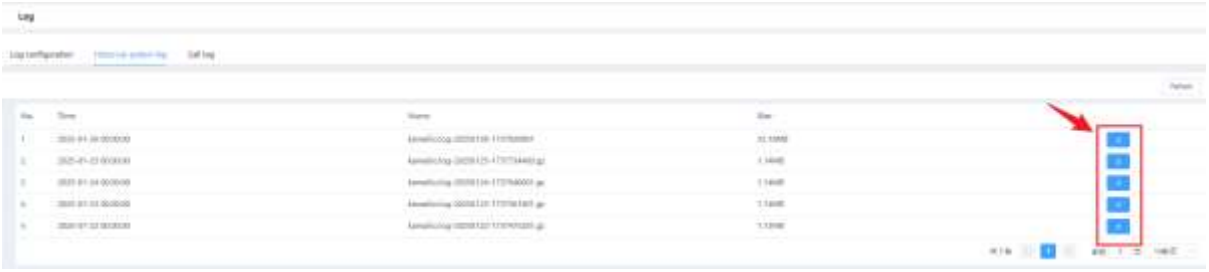


Figure 61 Historical System Log/Call Log

7.13.3 Backup and Recovery

Navigate to System Management > Backup & Restore, through which administrators can easily backup and restore system configurations, call logs, and other critical information to

 Copyright © Redstone Systems, Inc

prevent data loss or system failure.

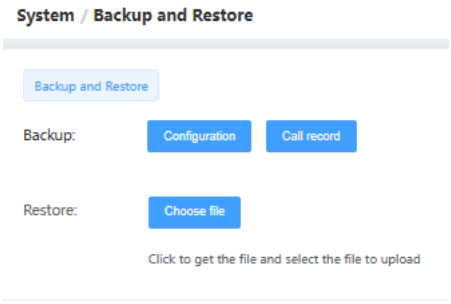


Figure62 Backup and Recovery

Table45 Backup and Recovery

Item	Definition
Data Backup	Used to back up the data of the current system, including configuration files, call logs, and to ensure that it can be restored in the event of a system failure.
Data Recovery	Used to restore system data from a backup file to ensure that the system is restored to the state it was in at the time of the backup.

7.13.4 Packetization

Navigate to System Management>Packet Capture, this function is used for fault analysis or problem localization, the captured packet is temporarily stored in dump.cap format, and can be downloaded for analysis after capturing stops. Press "Start" button to start the packet capture function.



Figure63 Data Grab Bag

 Copyright © Redstone Systems, Inc

7.13.5 Operation Log

Navigate to System Management > Operation Logs and the administrator can view the device operation logs.



Figure64 Operation Log

7.13.6 Alarm Log

Navigate to System Management > Alarm Logs, administrators can view the current device alarm logs, support filtering and set the log retention time.



Figure65 Alarm Log

8 Glossary

Letter	Nomenclature	Definition
A	AMR (Adaptive Multi-Rate Coding)	Adaptive Multi-Rate, an audio codec standard for speech compression.
A	API (Application Programming Interface)	An API is a set of rules and tools that allow different programs to interact with each other, enabling software developers to create applications that can connect to other applications or services.
C	CLI (Command Line Interface)	Command Line Interface for device configuration and management via the command line.
C	CQC (China Quality Certification Center)	China Quality Certification, the official quality certification organization in China.
C	CDR (Call Detail Record)	CDR is a system that records detailed information (e.g., call length, start and end times, participant numbers) about each call activity and is used to analyze call data and calculate charges.
D	DiffServ (Differentiated Services)	Differentiated Services, which manages network traffic by marking packets for prioritization.
D	DDoS (Distributed Denial of Service Attacks)	Distributed Denial of Service, a type of cyber attack that attacks a target system through multiple sources.
D	DoS (Denial of Service Attack)	Denial of Service, an attack that exhausts system resources through a large number of requests.
D	DTLS-SRTP (Datagram Transport Layer Security Protocol - Secure Real-Time Transport Protocol)	Datagram Transport Layer Security - Secure Real-Time Transport Protocol, a real-time data encryption protocol that combines DTLS and SRTP.

 Copyright © Redstone Systems, Inc

D	DTMF (Dual Tone Multi Frequency Mode)	Dual-Tone Multi-Frequency for key signal transmission, commonly used in telephone dialing and communication systems.
F	FSP (Field Safety Protocol)	FSP is a security protocol used to authenticate devices and ensure secure communication.
G	G.711 / G.723.1 / G.729a/b	Different voice coding standards ensure that the device is compatible with different communication systems and devices.
H	HA (High Availability)	High Availability, through dual-machine hot backup to improve system availability, to ensure that the system continues to run.
H	HTTP / HTTPS (Hypertext Transfer Protocol)	Hypertext Transfer Protocol / Hypertext Transfer Protocol Secure, used for network data transfer, HTTPS provides encrypted, secure transmission.
I	ICMP (Internet Control Message Protocol)	Used to convey control information in IP networks, often used to diagnose and manage networks.
I	IMS (IP Multimedia Subsystem)	IP Multimedia Subsystem, an IP-based multimedia service architecture that supports voice, video and multimedia communications
I	iLBC (Voice over Internet Protocol Low Bit Rate Codec)	internet Low Bitrate Codec, a codec for voice communication for low bandwidth environments.
J	Jitter Buffer	A buffer used at the receiving end to absorb jitter in network transmissions and ensure that voice data is continuous and smooth.
L	LDAP (Lightweight Directory Access Protocol)	LDAP helps computers find and manage people or device information such as e-mail addresses or printers on a network, and is commonly used for user and resource management within an organization.
M	MSRP (Message Session Relay Protocol)	Message Session Relay Protocol, a protocol used for instant messaging.
N	NGN (Next Generation Network)	Next Generation Network, a packet-switching-based network architecture designed to provide a variety of telecommunications services (including voice, data and multimedia services).
N	NAT (Network Address	Network Address Translation, used to translate

 Copyright © Redstone Systems, Inc

	Translation)	private IP addresses to public IP addresses, commonly used in routers and firewalls.
N	NTP / SNTP (Network Time Protocol / Simple Network Time Protocol)	Network Time Protocol / Simple Network Time Protocol for network time synchronization to ensure consistent time across all devices.
O	OPUS	An efficient voice and audio codec widely used in real-time communication.
R	RTP (Real Time Transport Protocol) / RTCP (Real Time Transport Control Protocol)	Real-Time Transport Protocol / Real-Time Control Protocol for real-time transmission of audio and video data, RTCP provides transmission control and statistics.
R	RESTful	Describes a style of network architecture that manipulates resources on the network via standard HTTP methods (e.g., GET, POST, PUT, DELETE), often used in the design of APIs to support expressive state transfer of resources.
S	SBC (Session Border Controller)	Session Border Controller, which provides call control and session management features to secure the network border.
S	SIP (Session Initiation Protocol)	Session Initiation Protocol for establishing, modifying and terminating multimedia sessions such as voice and video calls.
S	SRTP (Secure Real-Time Transport Protocol)	Secure Real-Time Transport Protocol for encrypting real-time audio and video data to ensure secure communications.
S	SSH (Secure Shell Held Protocol)	Secure Shell, encrypted command line interface management for secure remote access.
S	SSL (Security Layer Agreement)	SSL is a security protocol used to establish an encrypted connection over a computer network to ensure the security of data as it travels between the server and the client.
T	TLS (Transport Layer Security protocol)	Transport Layer Security, which secures data by encrypting transport layer data.
T	TCP (Transmission Control Protocol)	TCP is a network protocol that ensures that packets are transmitted accurately and without error through an acknowledgement and retransmission mechanism, and is suitable for

 Copyright © Redstone Systems, Inc

		applications that require high reliability, such as e-mail and file transfers.
U	UDP (User Datagram Protocol)	UDP is a fast network transport protocol that does not guarantee packet order or integrity, and the unit of transmission for UDP is called a "datagram". It is used for video streaming and online gaming, where speed is more important than transmission reliability.
V	VLAN (Virtual Local Area Network)	Virtual Local Area Network, used to divide the network into logical segments for network isolation and traffic management.
V	VGA (Video Graphics Array)	Video Graphics Array, an interface for display output.

 Copyright © Redstone Systems, Inc