SX10000-S Session Border Controller

Administrator's Manual

Document version: 2025-01

Published: 2025-01-24

Copyright© New Rock Technologies, Inc. 2025. All rights reserved.

Without the written permission of the Company, any unit or individual may not extract or copy part or all of the contents of this document without authorization, and may not be disseminated in any form.

Website: https:/en.newrocktech.com/

Documentation Center: https://en.newrocktech.com/DocumentCenter

Tel：021-61202700

Fax: 021-61202704

1 Contents

1 CONTENTS 1
2 ABOUT THIS DOCUMENT 9
3 APPLICATION SCENARIOS 10
4 NETWORK TOPOLOGY 12
5 PRODUCT SPECIFICATIONS 13
5.1 PRODUCT OVERVIEW 13
5.2 FUNCTIONS AND APPLICATIONS 13
5.2.1 Functional Features 14
5.2.2 Functional Module 16
5.2.2.1 Call Processing Module 16
5.2.2.2 Safety Module 17
5.2.2.3 Management Module 18
5.3 NORM 19
5.3.1 Performance Parameters 19
5.3.2 Management and Monitoring 21
5.3.3.1 Management Tools 21
5.3.3.2 Remote Management 21
6 SOFTWARE INSTALLATION 22
7 CONFIGURING THE SBC ADMINISTRATOR BACKEND 24
7.1 OPERATOR GROUP 24
7.1.1 IP certification 24
7.1.2 User Name/Password Authentication 30
7.2 PBX 32
7.3 DOMAIN MANAGEMENT 37
7.4 INBOUND SIGNALING 38

 Copyright© New Rock Technologies, Inc.

7.4.1 Number Routing 38
7.4.2 Domain Name Routing 39
7.5 ROUTING 40
7.5.1 Number Routing 40
7.5.2 Domain Name Routing 41
7.6 CALL TRACKING 41
7.7 NETWORK MANAGEMENT 43
7.7.1 Network Setup 43
7.7.2 Port Configuration 45
7.8 TERMINAL RECORDS 46
7.9 CALL RECORD 47
7.10 TEMPLATE MANAGEMENT 48
7.10.1 Call black and white list templates 48
7.10.2 DTMF Templates 49
7.10.3 Call Frequency Templates 49
7.10.4 Media Codec Templates 50
7.10.5 Routing Effective Time Template 51
7.10.6 Number Change Template 52
7.11 APPLICATION CONFIGURATION 53
7.11.1 SIP Configuration 53
7.11.2 Media Configuration 54
7.11.3 Call Configuration 55
7.11.4 Call Black/White List 56
7.12 SECURITY MANAGEMENT 57
7.12.1 WEB Defense 57
7.12.2 SSH Defense 58
7.12.3 SIP Defense 59
7.12.4 Other Defenses 60
7.12.5 Access to black and white lists 60
7.13 SYSTEM MANAGEMENT 61

 Copyright© New Rock Technologies, Inc.

7.13.1 System Configuration 61
7.13.2 Log Management 61
7.13.3 Backup and Recovery 62
7.13.4 Packetization 63
7.13.5 Operation Log 63
7.13.6 Alarm Log 64

8 GLOSSARY 65

Contents of Figures

Figure1 SX10000-S Application Scenarios Figure 1 10
Figure2 SX10000-S Application Scenarios Figure 2 11
Figure3 SX10000-S Application Scenario Figure 3 11
Figure4 SX10000-S networking topology 12
Figure5 SBC Backend Login Screen 24
Figure6 IP Authentication Interface 25
Figure7 Fill in the group name 26
Figure8 Edit Operator Group 26
Figure9 Adding Operator Group Details 27
Figure10 Delete Endpoints 29
Figure11 Refresh Node 29
Figure12 Filtering Users 30
Figure13 Selecting an Outgoing Interface 30
Figure14 Download Template 31
Figure15 Bulk Modify/Delete Username Password Authentication 31
Figure16 Filtering the PBX 32
Figure17 Add PBX Details 33
Figure18 Add PBX Details 2 33
Figure19 New Endpoints 34
Figure20 refreshes the list 36
Figure21 Filter list by type 36
Figure22 Edit/Delete Endpoint Information 36
Figure23 New Domain 37
Figure24 Filter Fields 38

 Copyright© New Rock Technologies, Inc.

Figure25 number routing 38
Figure26 Domain Name Routing 39
Figure27 Number Routing 40
Figure28 Edit/Delete 40
Figure29 Adding a Domain Route 41
Figure30 Call Tracking 41
Figure31 Reserved Timing Configuration 42
Figure32 Network Settings 43
Figure33 Network Setup 2 44
Figure34 New listening port 45
Figure35 encryption algorithm 46
Figure36 Terminal Records 46
Figure37 Call Log 47
Figure38 New Template 48
Figure39 New DTMF template 49
Figure40 Call Frequency Template 49
Figure41 Media Codec Template 50
Figure42 Routing Effective Time Template 51
Figure43 Number Change Template 52
Figure44 SIP Configuration 53
Figure45 Media Configuration 54
Figure46 Call Configuration 55
Figure47 Call Black/White List 56
Figure48 WEB DEFENSE 57
Figure49 SSH Defense 58
Figure50 SIP Defense 59
Figure51 Other defenses 60
Figure52 Accessing the Black and White List 60

Figure53 System Configuration 61

Figure54 Log Management 61

Figure 55 Historical System Log/Call Log 62

Figure56 Backup and Recovery 62

Figure57 Data Grab Bag 63

Figure58 Operation Log 63

Figure59 Alarm Log 64

Content of Tables

Table1 SX10000-S Performance Parameters 19
Table2 Supported Codecs 20
Tables3 Management Tools 21
Table4 IP Certification 28
Table5 Add Username/Password Authentication 31
Table6 New PBX 33
Table7 New Endpoints 34
Table8 New field 37
Table9 Number Routing 38
Table10 Domain Name Routing 39
Table11 Number Routing 40
Table12 Add Domain Routing 41
Table13 Call Tracking 42
Table14 Network Settings 43
Table15 Network Settings 44
Table16 Port Configuration 45
Table17 Global Configuration 45
Table18 Encryption Algorithm 46
Table19 Call Log 47
Table20 New Template 48
Table21 New DTMF template 49
Table22 Call Frequency Template 50
Table23 Media Codec Template 50
Table24 Routing Effective Time Template 51

 Copyright© New Rock Technologies, Inc.

Table25 Change of Number Template 52
Table26 SIP Configuration 53
Table27 Media Configuration 54
Table28 Call Configuration 55
Table29 Call Black/White List 57
Table30 WEB DEFENSE 57
Table31 SSH Defense 58
Table32 SIP Defense 59
Table33 Other Defense 60
Table34 Access to Black and White Lists 61
Table35 Log Levels 62
Table36 Backup and Recovery 63

2 About this Document

This manual is designed to provide detailed parameter descriptions and operating instructions for administrators who use and manage the SX10000-S session border controller. It includes technical descriptions of the SX10000-S, installation procedures, configuration instructions, maintenance strategies, and solutions to common problems.

 Copyright© New Rock Technologies, 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 SX10000-S 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 SX10000-S 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.

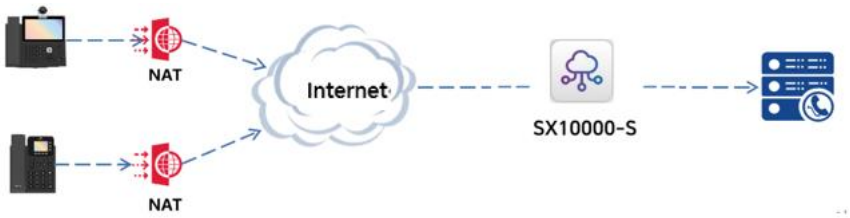


Figure1 SX10000-S Application Scenarios Figure 1

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

 Copyright© New Rock Technologies, Inc.

non-trusted networks with each other. When interconnecting, issues such as network topology concealment, media aggregation and forwarding, and security must be considered. the SX10000-S 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.

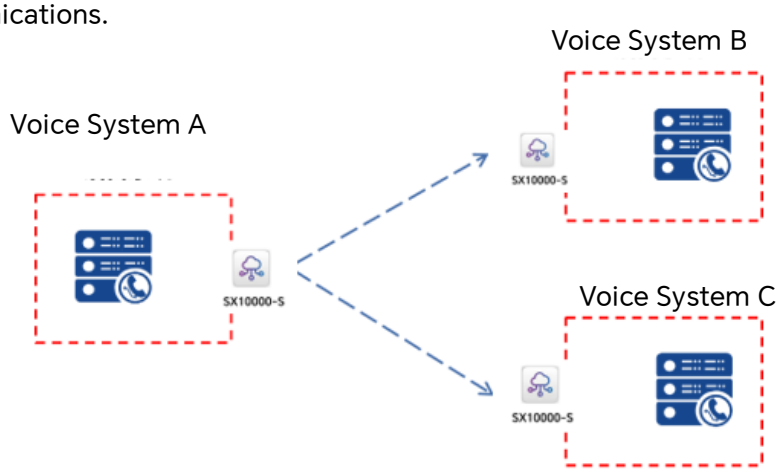


Figure2 SX10000-S Application Scenarios Figure 2

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. SX10000-S can effectively adapt to the devices of different vendors in such scenarios to ensure efficient compatibility and organic integration of multi-vendor equipment environment.

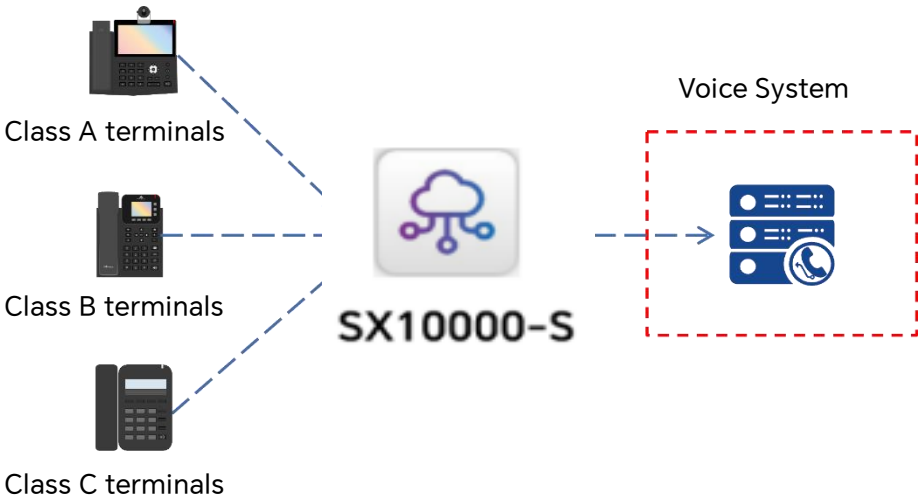


Figure3 SX10000-S Application Scenario Figure 3

4 Network Topology

Figure 4 illustrates a typical networking topology for the SX10000-S session border controller in an enterprise network. This topology includes the internal communication system, the SX10000-S session border controller, and the external communication system.

The topology map includes the following components:

- Internal Communication System: On the left, the SX10000-S connects to internal IP phones and servers within the organization, ensuring secure and efficient internal communications.
- SX10000-S 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 SX10000-S 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.

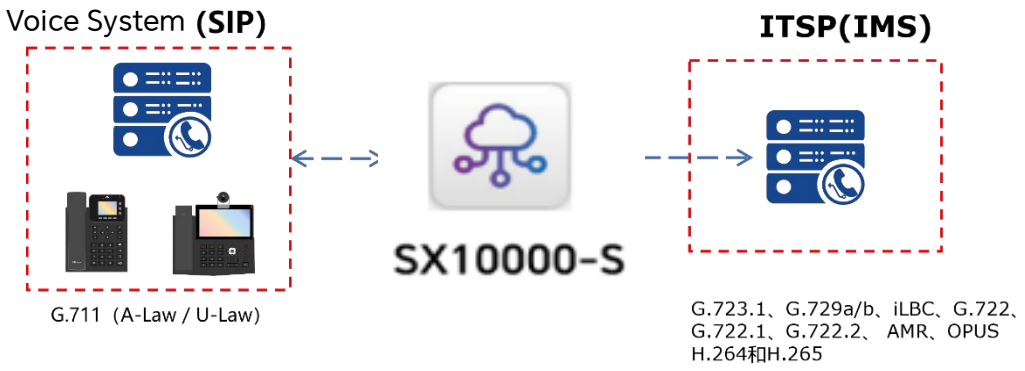


Figure4 SX10000-S networking topology

5 Product Specifications

Performance and reliability are key factors when selecting and deploying enterprise communications equipment. The SX10000-S Session Border Controller delivers high performance and flexibility with a variety of advanced features. The devices support multi-user concurrent sessions and provide high-quality voice and video communications. By utilizing advanced encryption and security measures, the SX10000-S ensures the confidentiality and integrity of communications. In addition, a user-friendly management interface simplifies daily operation and maintenance.

5.1 Product Overview

Designed for small and medium-sized businesses, the SX10000-S 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 SX10000-S 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 SX10000-S Session Border Controllers and their applicability in different application scenarios. The SX10000-S 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.

 Copyright© New Rock Technologies, Inc.

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: SX10000-S is perfectly compatible with IMS system and supports flexible routing rule settings to adapt to different network environments and application scenarios.
- ✓ User Support: The SX10000-S supports up to 20000 user registrations and is capable of handling 2000 concurrent sessions .
- ✓ 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 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-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: SX10000-S 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 SX10000-S 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 SX10000-S 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: SX10000-S devices support proxy registration and forwarding registration functions for terminal devices, ensuring that terminal devices are authenticated and registered in different network environments. 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 SX10000-S 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.

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.

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.

5.3 Norm

This section describes in detail the various specification parameters of the SX10000-S 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 SX10000-S and serves as a reference for configuration and deployment.

5.3.1 Performance Parameters

Table1 SX10000-S Performance Parameters

Performance indicators	Descriptive
Maximum number of concurrent sessions	2000 concurrent routes
Call processing power (CPS)	90 calls per second
Number of user registrations	Supports up to 20000 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

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.

 Copyright© New Rock Technologies, Inc.

5.3.2 Management and Monitoring

This section describes the management and monitoring tools for the SX10000-S Session Border Controller, as well as the remote management features and how to use them.

5.3.3.1 Management Tools

Tables3 Management Tools

Item	Definition
SSH	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 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 SX10000-S 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© New Rock Technologies, Inc.

6 Software Installation

Supported Operating Systems

Architecture	Operating System	Version Information	Kernel Version
x86_64	CentOS	CentOS 7	Default kernel
x86_64	Ubuntu Server	22.04.4 LTS	5.15.0-107-generic
x86_64	UOS Server	20 1070a	4.19.0-91.82.179.uelc20.x86_64

Prerequisites:

- The network environment must remain uninterrupted, and ensure that DNS services are enabled.
- The deployed dual-machine system must maintain consistent timing.

I. Uninstall the old version (if present)

Before installing the new version, please verify whether an older version is present. If it is installed, follow these steps to complete the uninstallation:

Step 1 Uninstall the Keepalived component:

```
sbc uninstall -kpa
```

Step 2 Uninstall SBC and the database:

```
sbc uninstall -all
```

Note If the process becomes stuck during uninstallation, you can temporarily disable the firewall and then re-execute the command.

Step 3 Delete residual directories: Navigate to /opt/ and remove the SBC directory;

II. Install the new version

Step 1 Upload the new version installation package (tar) to the /opt directory.
Step 2 Unzip and navigate to the installation directory, then run the installation script.

 Copyright© New Rock Technologies, Inc.

```
./install.sh
```

 If you encounter any issues during installation (such as network unavailability), you can disable your firewall and then run the installation again.

III. Set Web Login Password

After installation is complete, you need to configure the administrator account and password for the web management interface. Execute the following command via the command line:

```
sbc setcredentials -dc admin:New Password
```

Example: (Set the username to admin and the password to admin)

```
sbc setcredentials -dc admin:admin
```

7 Configuring the SBC Administrator Backend

Log in to the SBC administrator backend

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

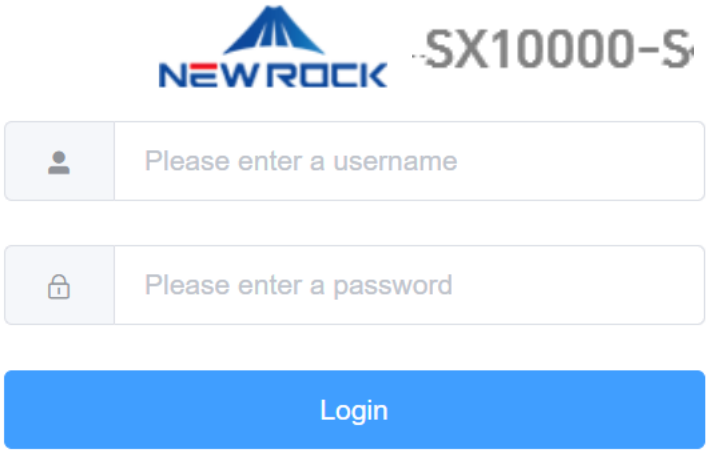


Figure5 SBC Backend Login Screen

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 SBC, 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.

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.

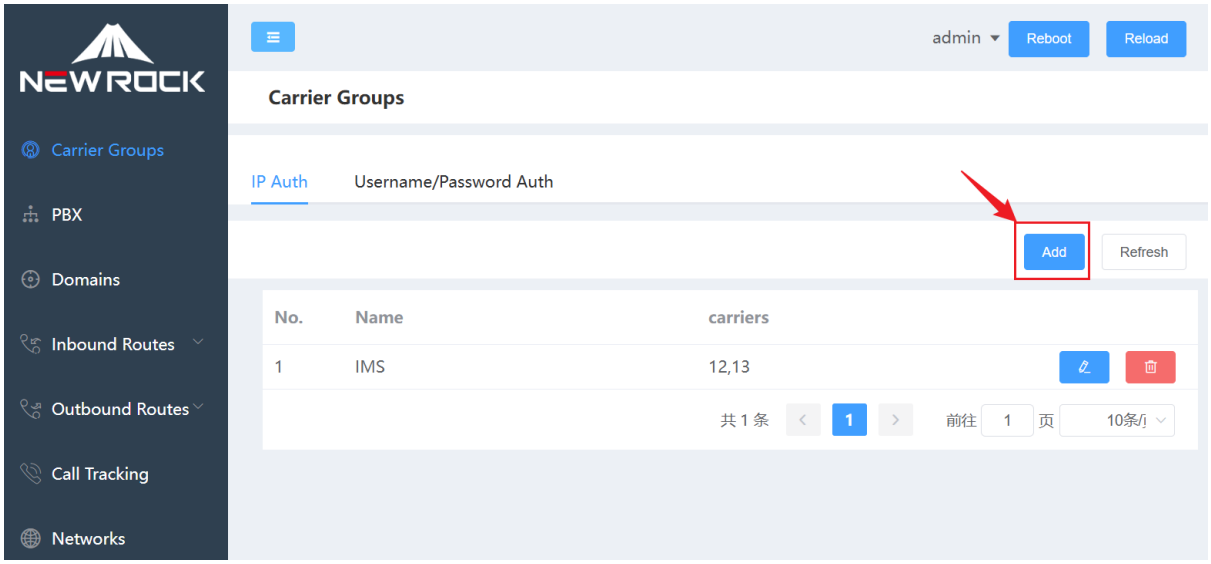
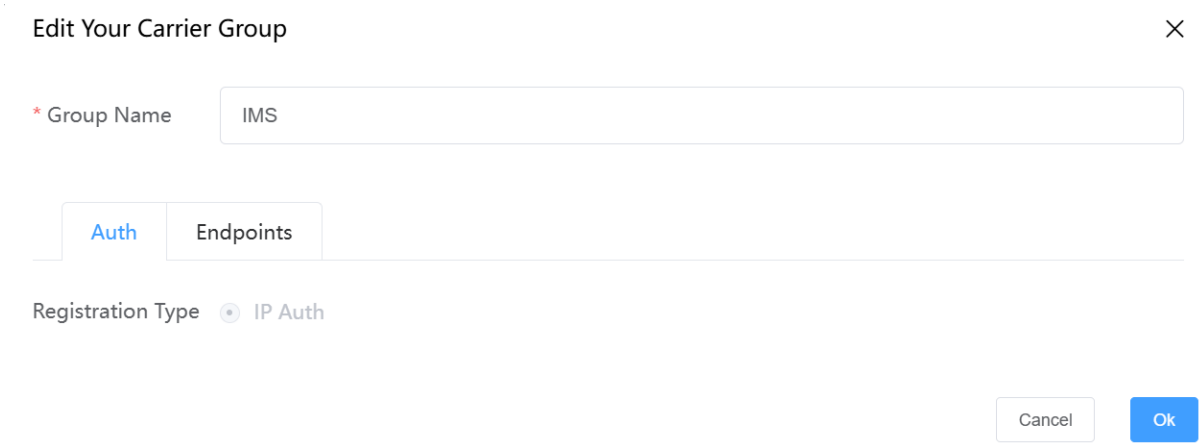
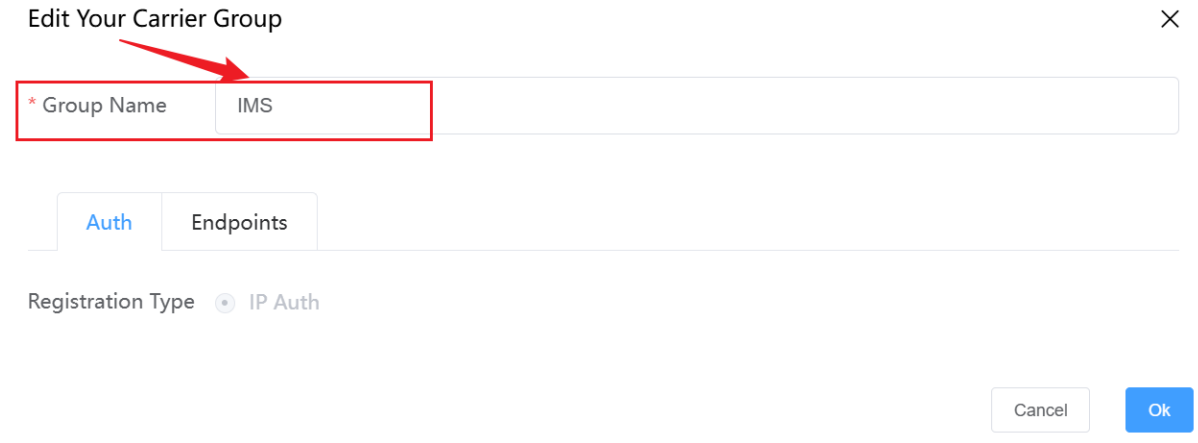


Figure6 IP Authentication Interface

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



Step.2 Fill in the group name



 Copyright© New Rock Technologies, Inc.

Figure7 Fill in the group name

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

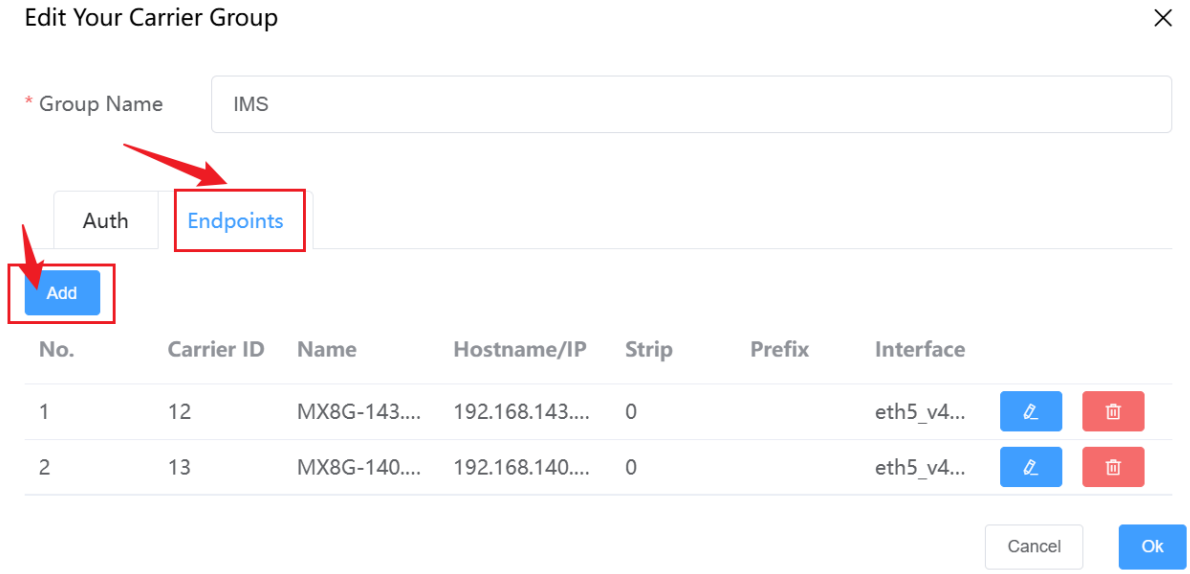


Figure8 Edit Operator Group

 Copyright© New Rock Technologies, Inc.

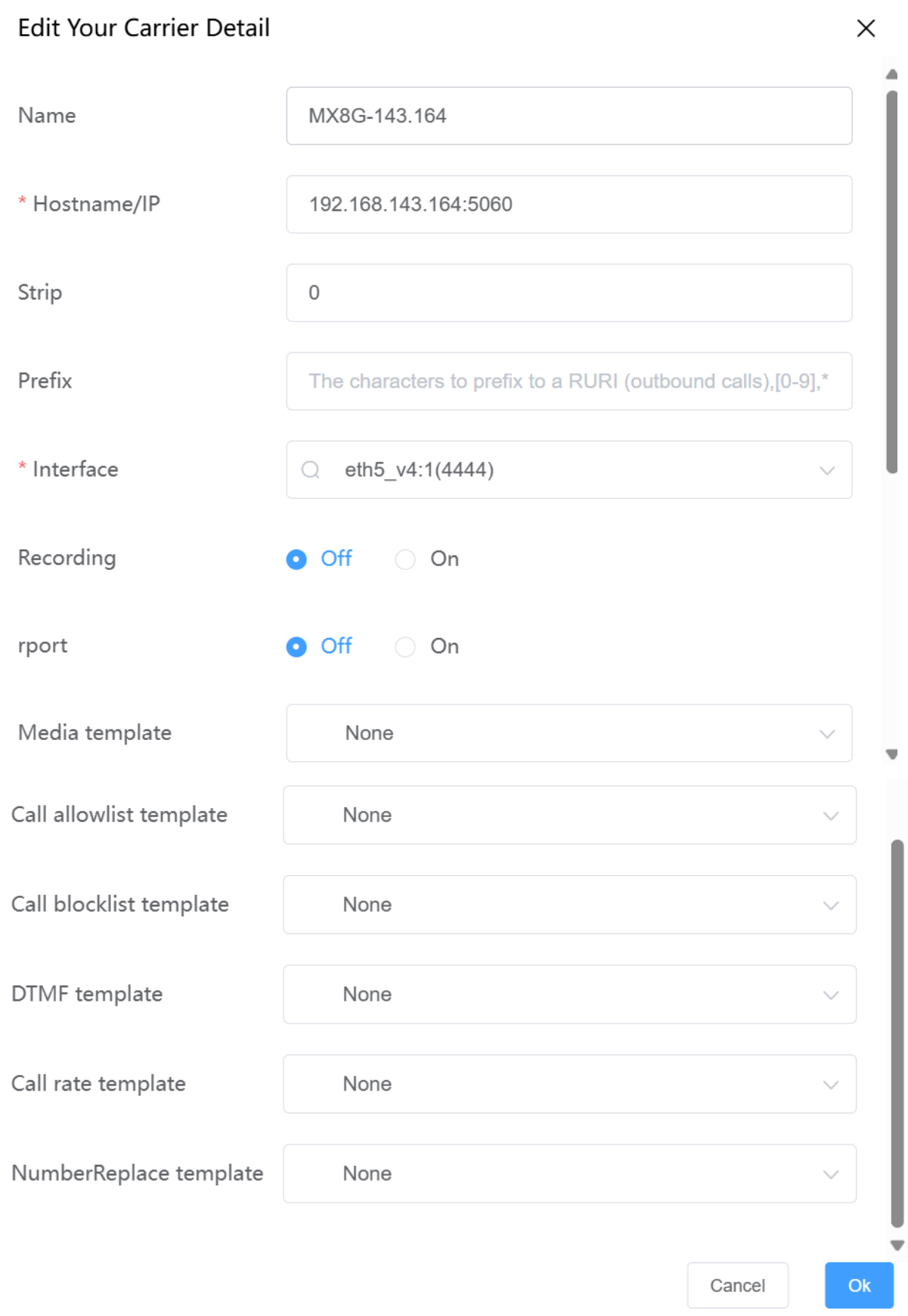


Figure9 Adding Operator Group Details

 Copyright© New Rock Technologies, Inc.

Table4 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© New Rock Technologies, 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.

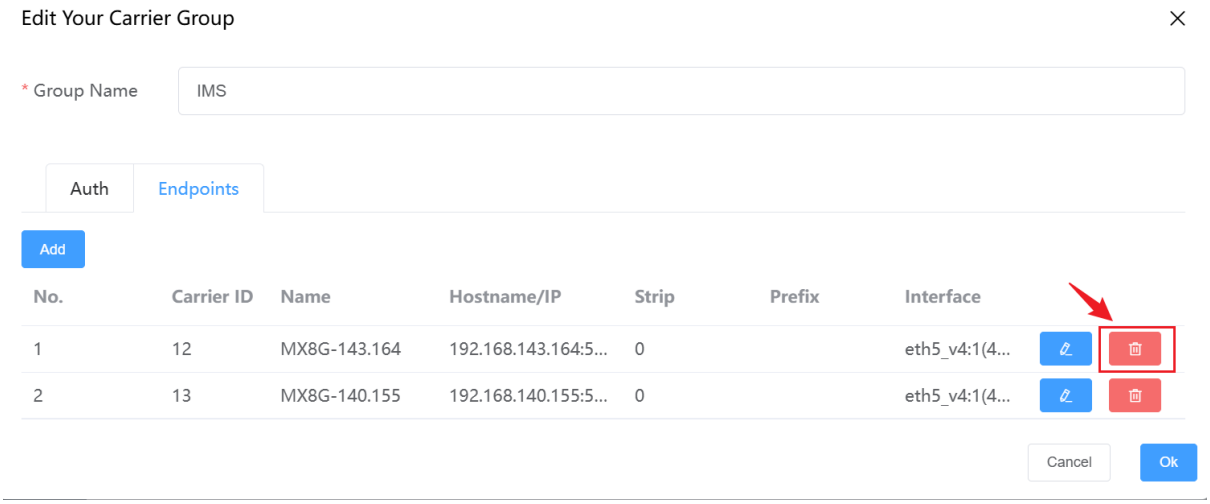


Figure10 Delete Endpoints

Refresh Node

Click Refresh to refresh the node information.

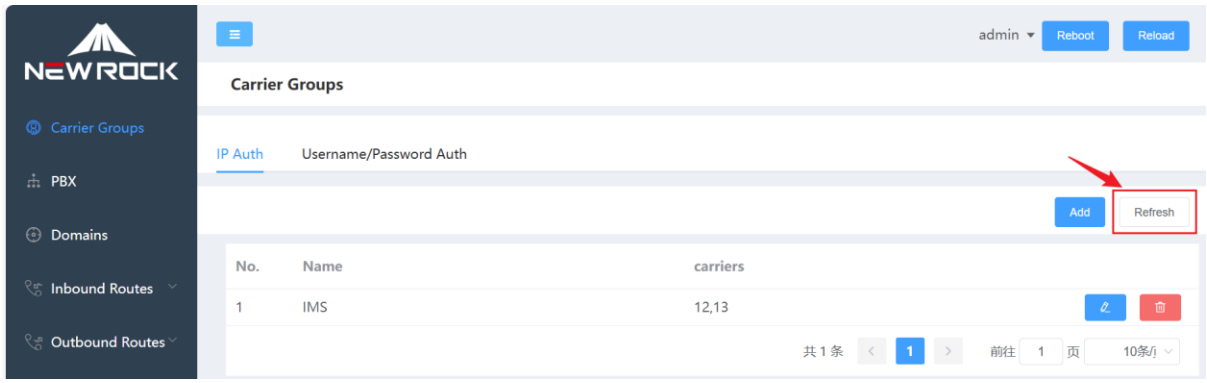


Figure11 Refresh Node

7.1.2 User Name/Password Authentication

Filtering Users

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

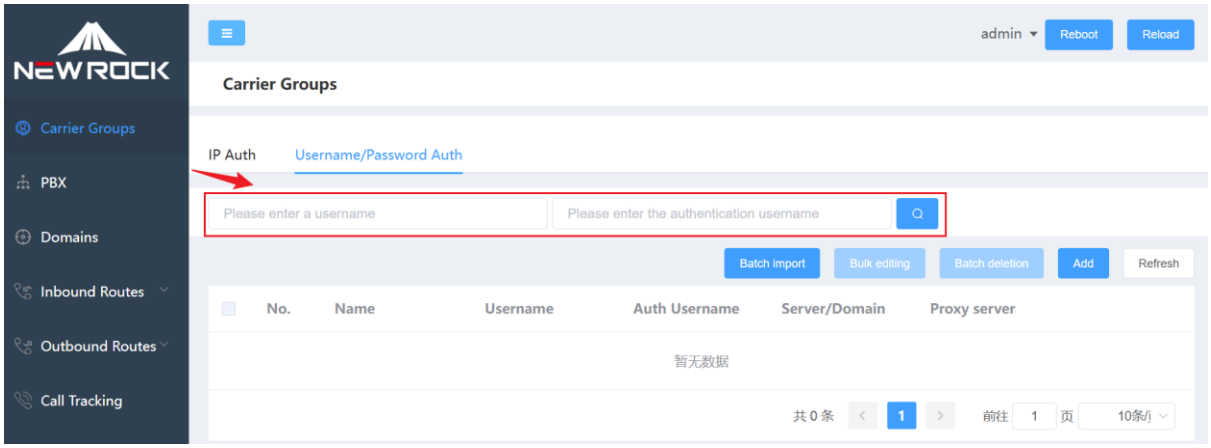


Figure12 Filtering Users

Batch Import

SBC supports batch import of operator groups.

Step.1 Select Outgoing Interface

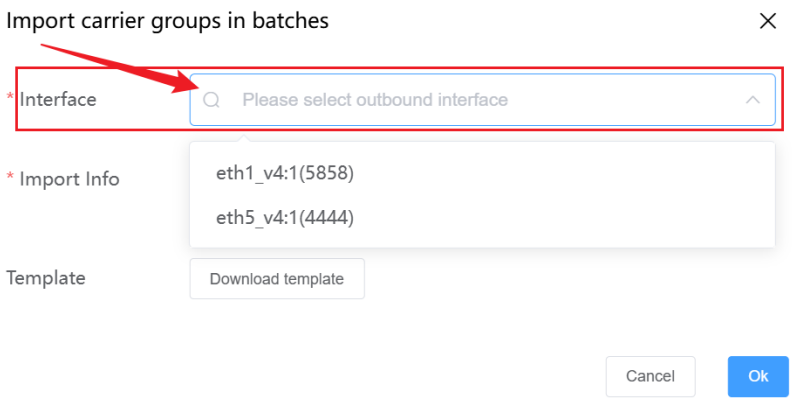


Figure13 Selecting an Outgoing Interface

Step.2 Importing information

Download Templates

Click Download Templates to download an import information template.

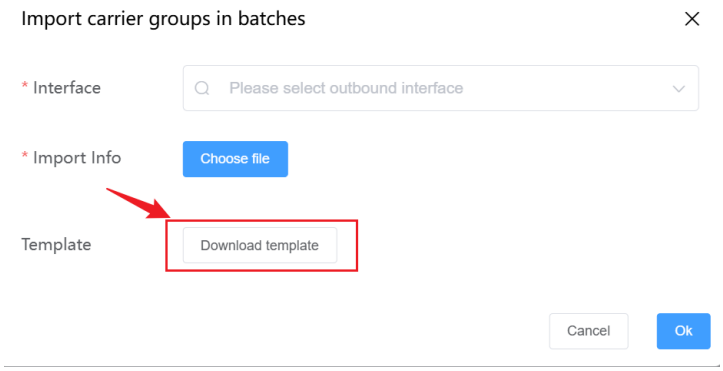


Figure14 Download Template

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.

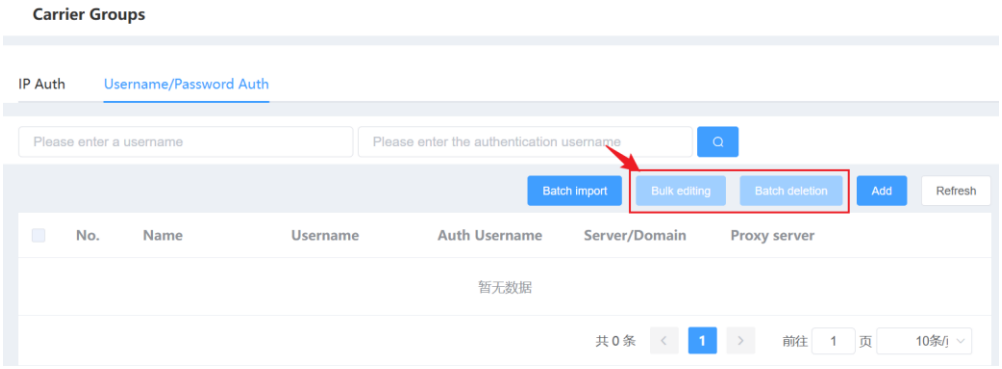


Figure15 Bulk Modify/Delete Username Password Authentication

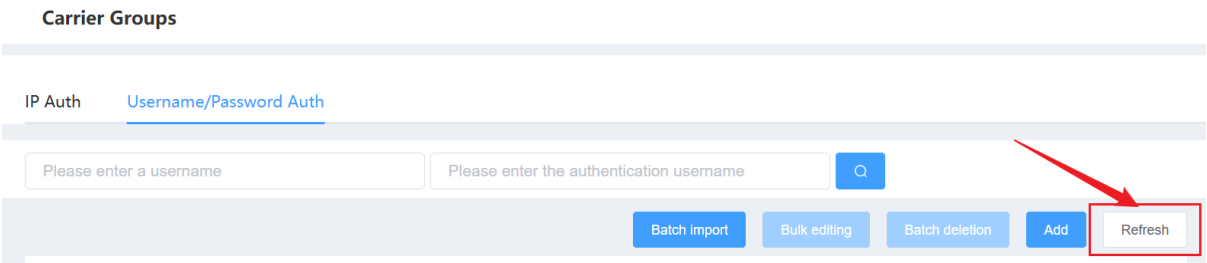
Add username/password authentication

Table5 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 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



7.2 PBX

Screening PBX

Enter a name/username to filter PBX devices.

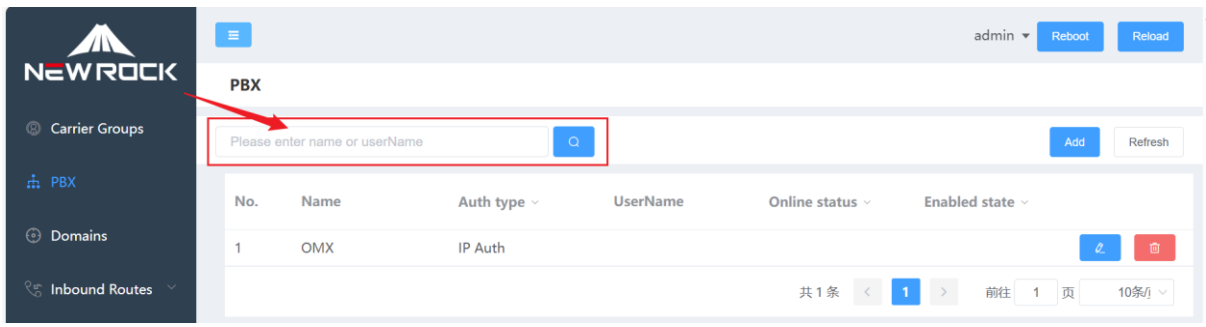


Figure16 Filtering the PBX

Add PBX details

Navigate to PBX and click Add to add PBX details.

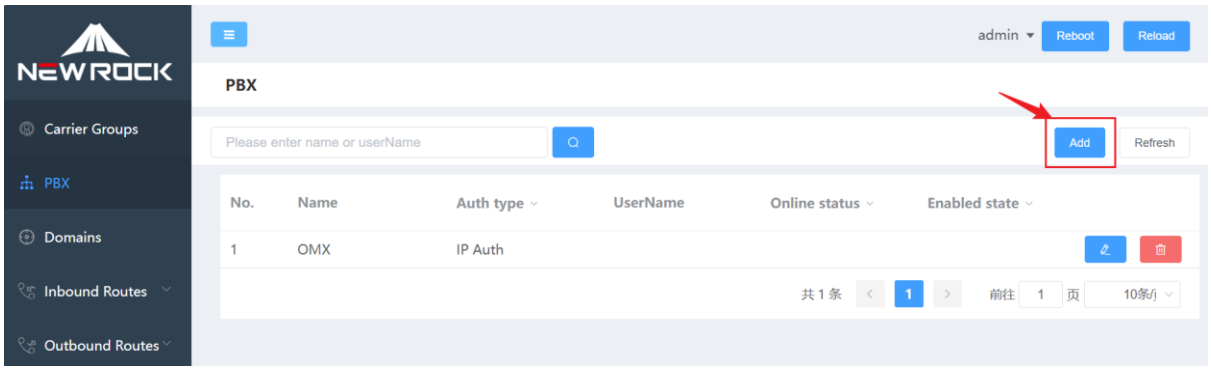


Figure17 Add PBX Details

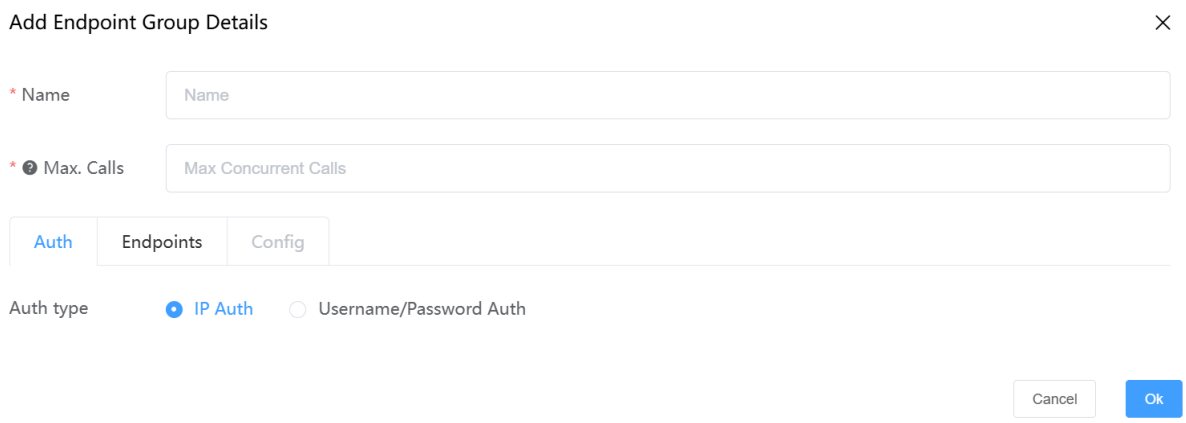


Figure18 Add PBX Details 2

Table6 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.

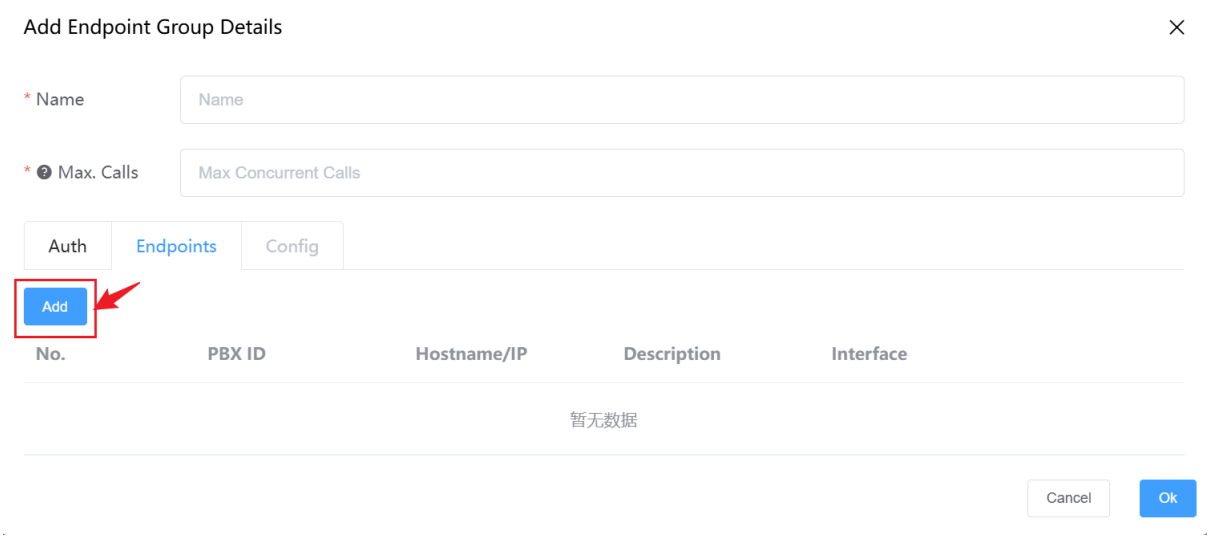


Figure19 New Endpoints

Table7 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 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.

 Copyright© New Rock Technologies, Inc.

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© New Rock Technologies, Inc.

Refresh List

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

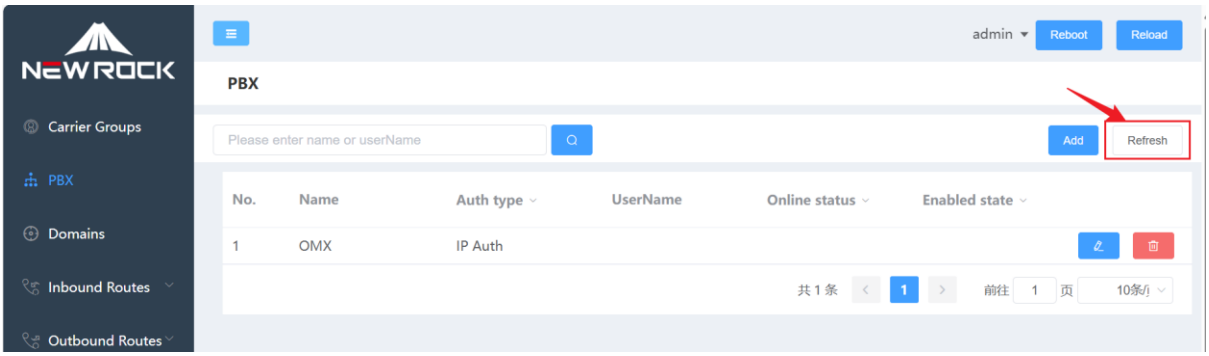


Figure20 refreshes the list

Filter List by Type

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

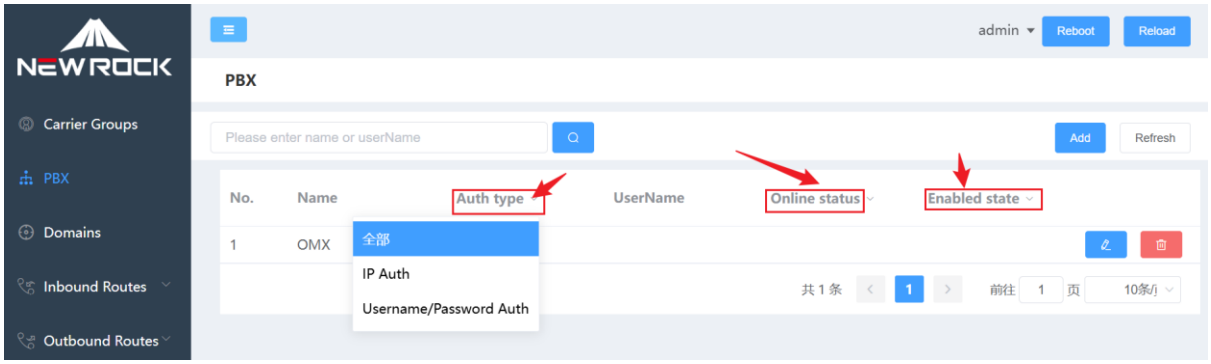


Figure21 Filter list by type

Edit/Delete Endpoint Information

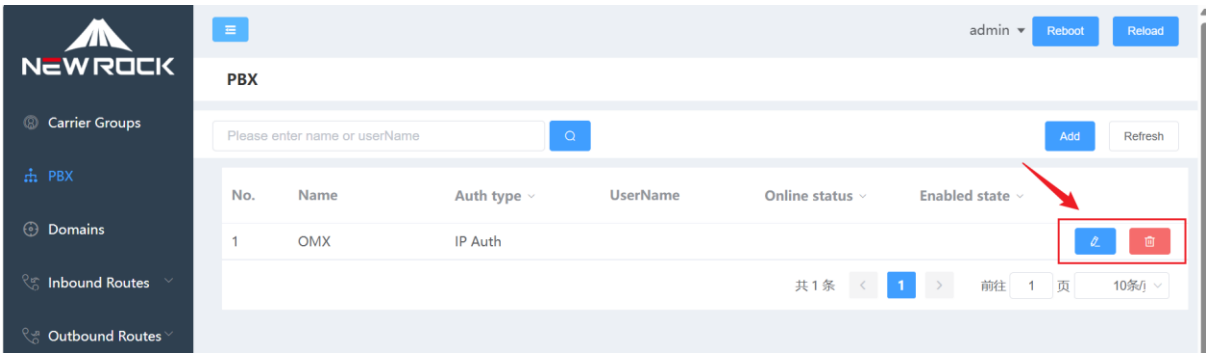


Figure22 Edit/Delete Endpoint Information

7.3 Domain Management

New Domain

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

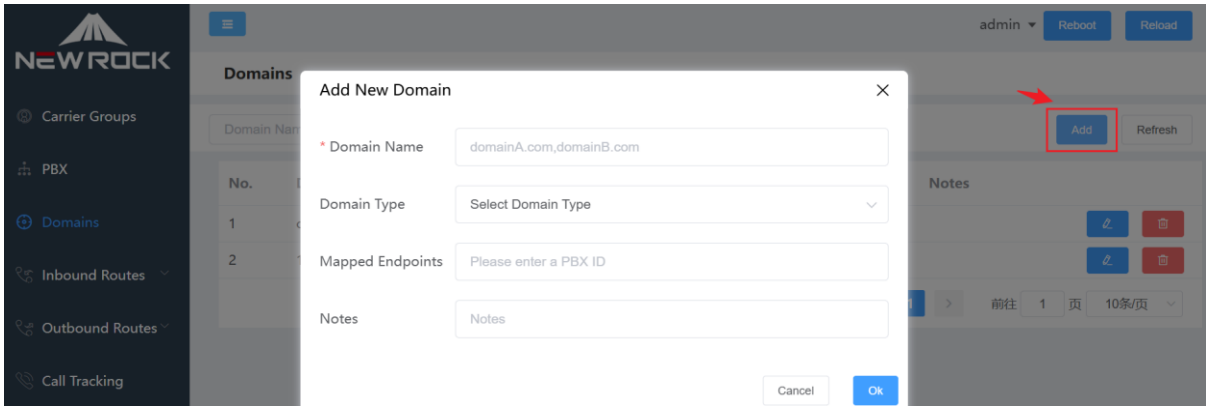


Figure23 New Domain

Table8 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.

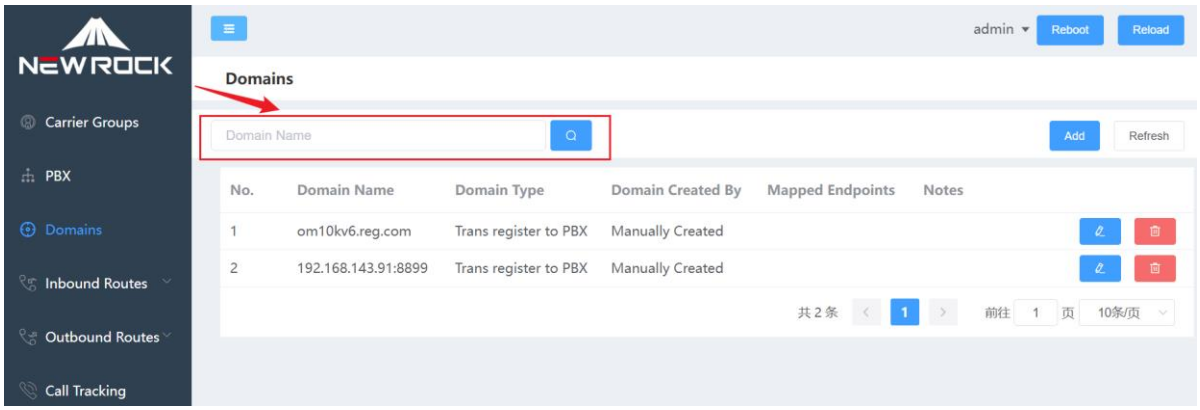


Figure24 Filter Fields

7.4 Inbound Signaling

7.4.1 Number Routing

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

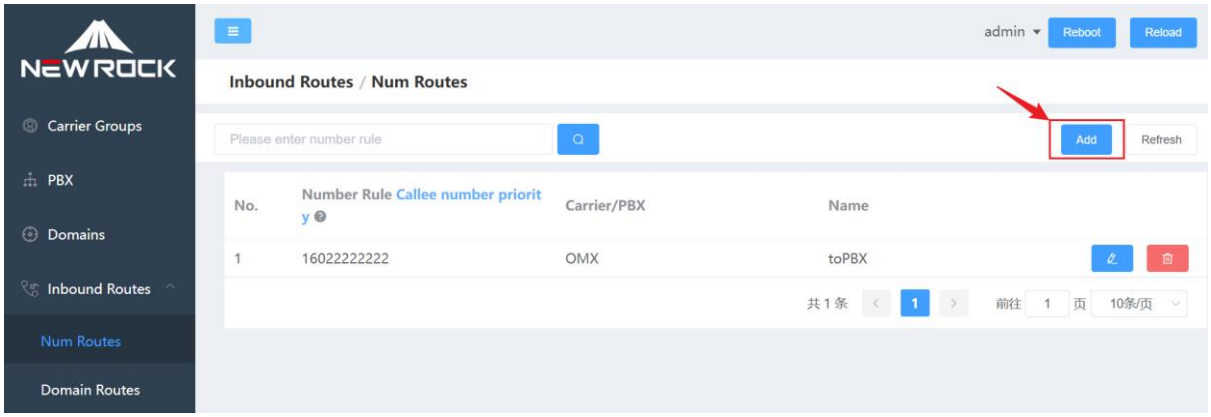


Figure25 number routing

Table9 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)

7.4.2 Domain Name Routing

Click New to add a new domain route.

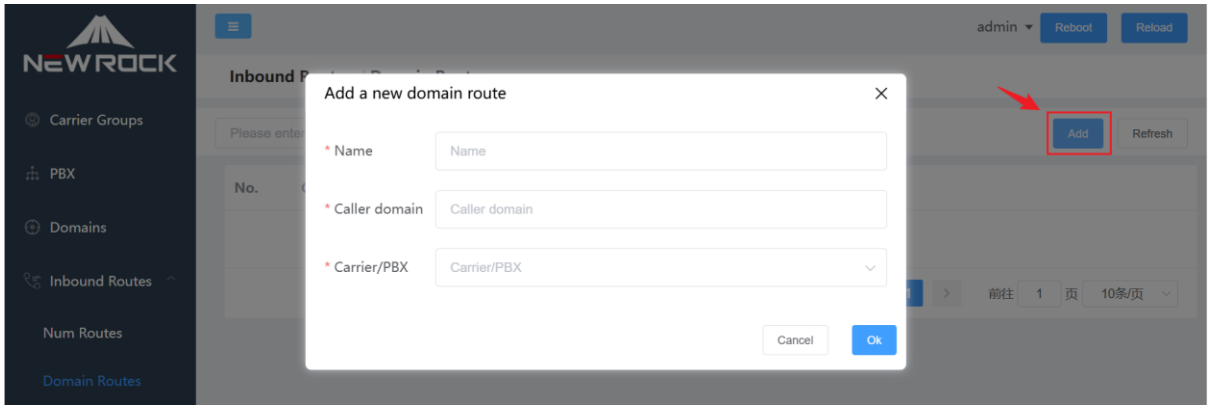


Figure26 Domain Name Routing

Table10 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)

 Copyright© New Rock Technologies, Inc.

7.5 Routing

7.5.1 Number Routing

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

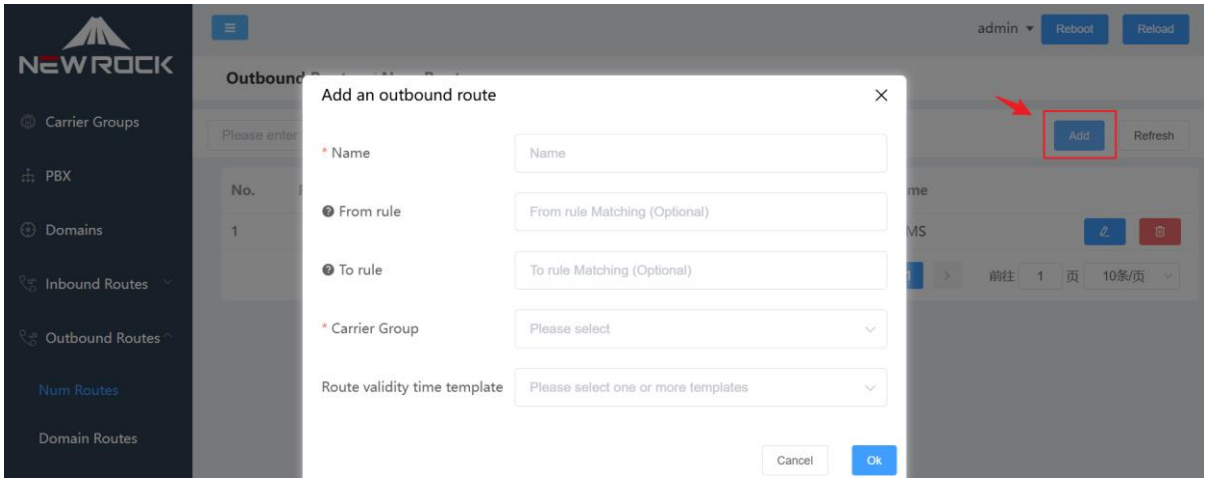


Figure27 Number Routing

Table11 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.

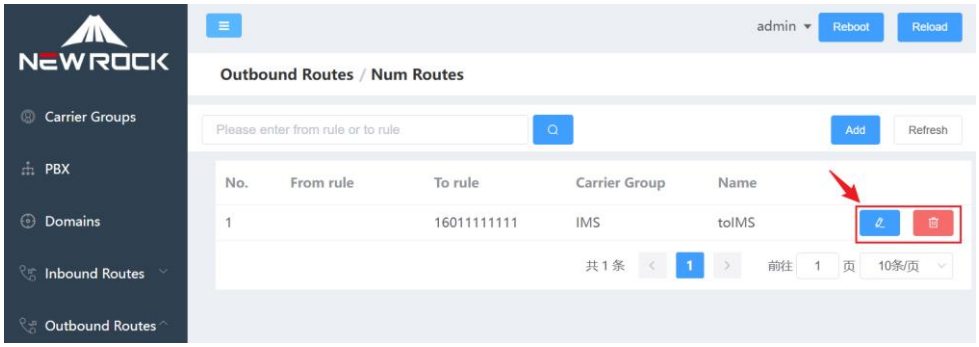


Figure28 Edit/Delete

7.5.2 Domain Name Routing

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

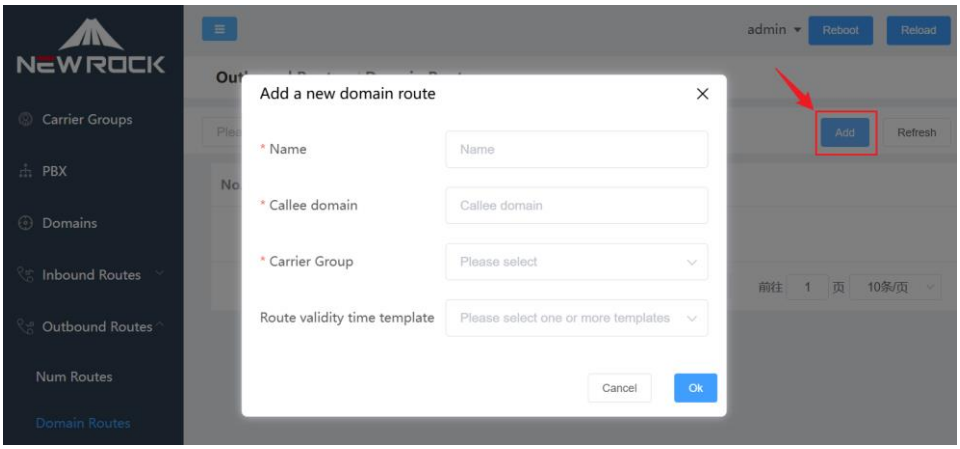


Figure29 Adding a Domain Route

Table12 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.

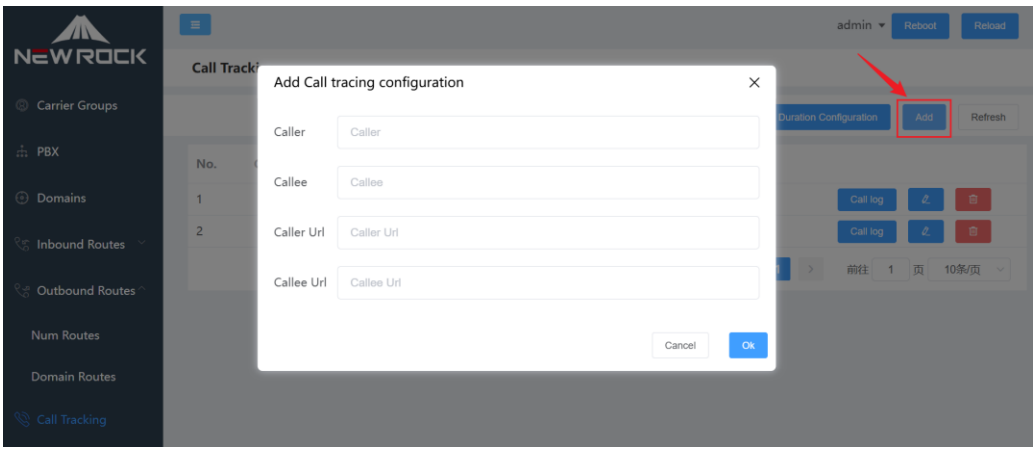


Figure30 Call Tracking

Table13 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.

Retained time-configuration

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

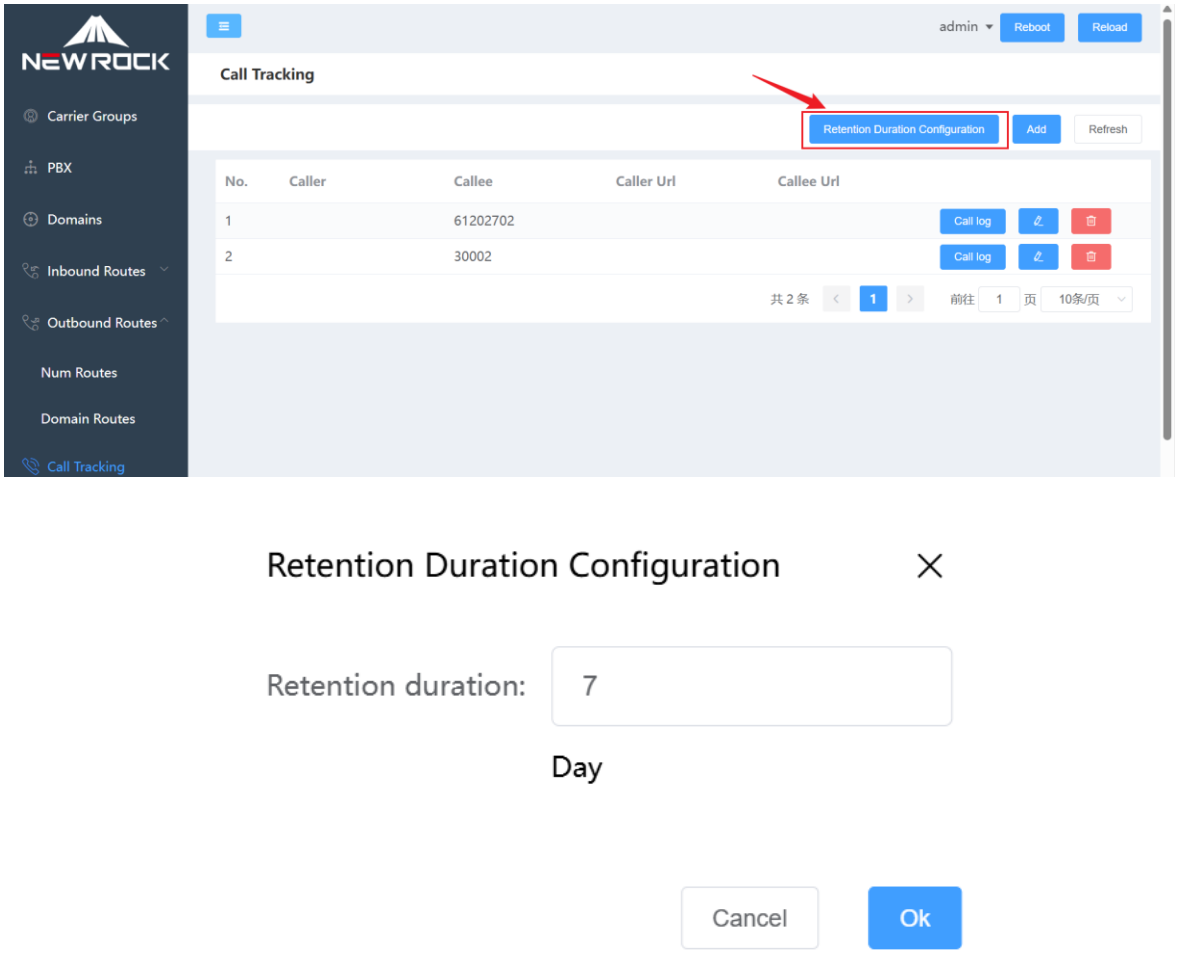


Figure31 Reserved Timing Configuration

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.

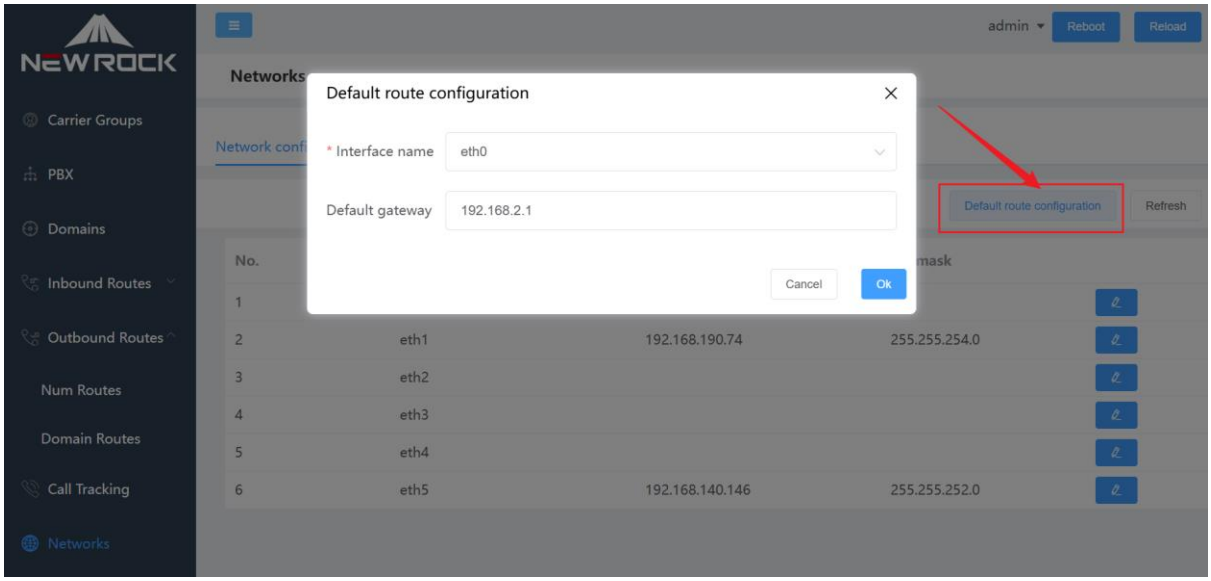


Figure32 Network Settings

Table14 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.

 Copyright© New Rock Technologies, Inc.

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.

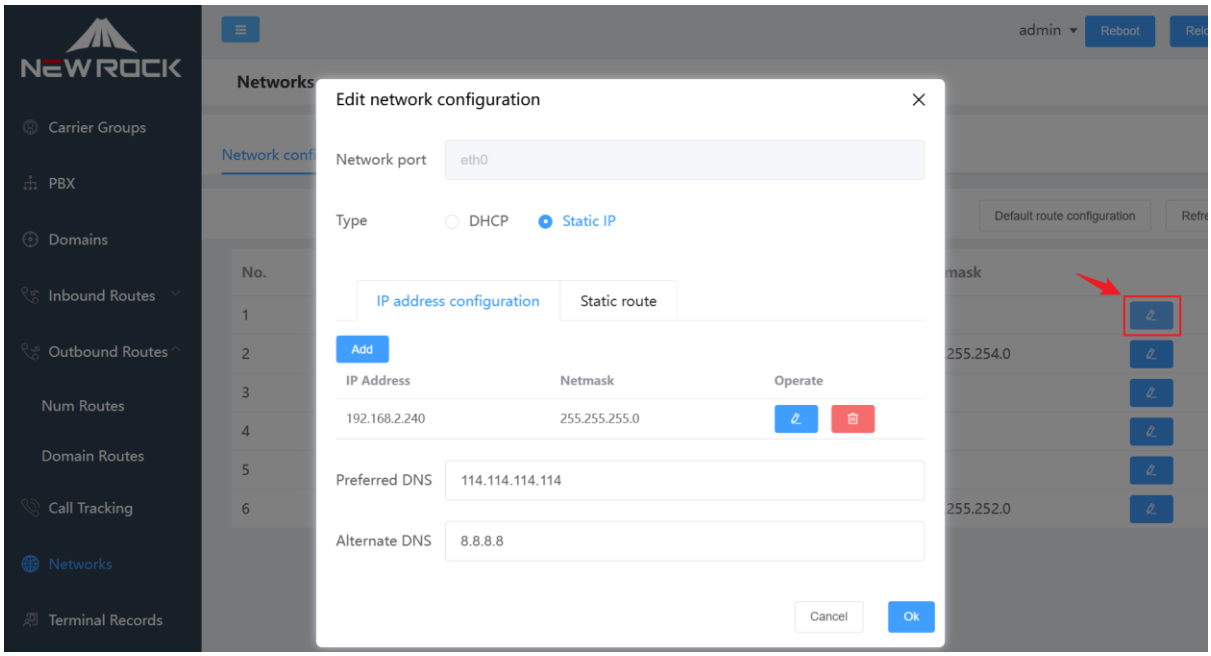


Figure33 Network Setup 2

Table15 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© New Rock Technologies, Inc.

7.7.2 Port Configuration

New listening port

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

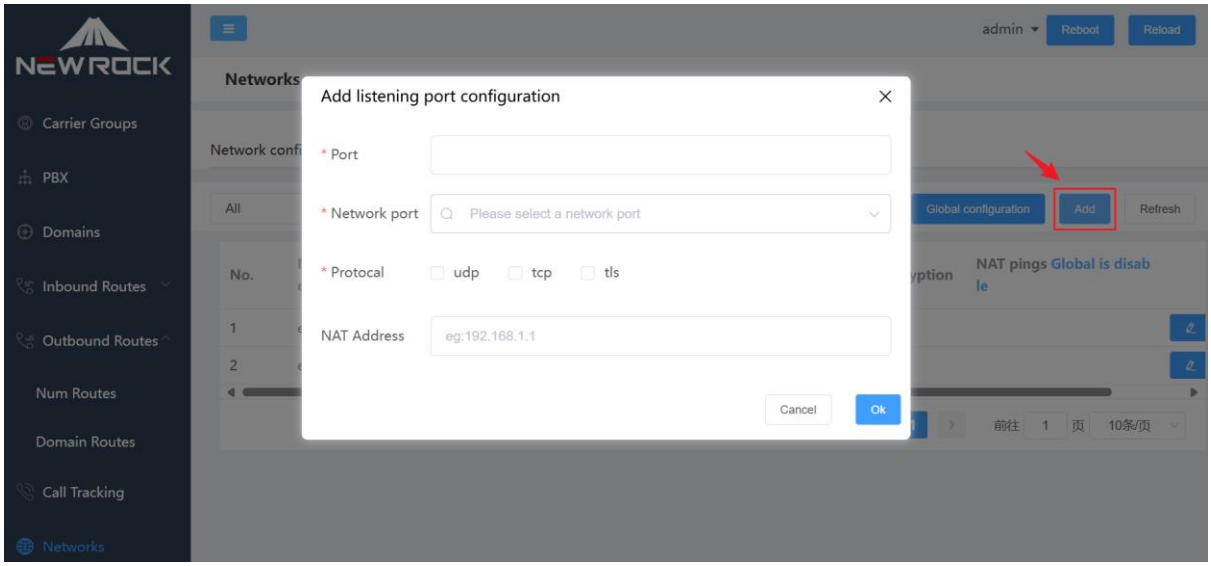


Figure34 New listening port

Table16 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.

Global configuration

Table17 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.

Table18 Encryption Algorithm

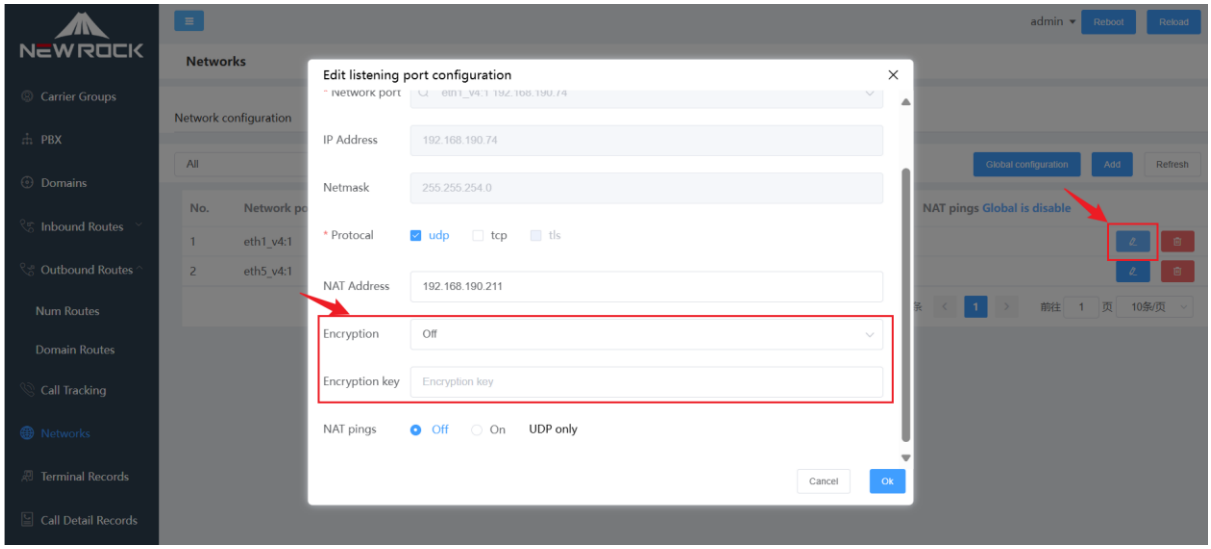


Figure35 encryption algorithm

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.

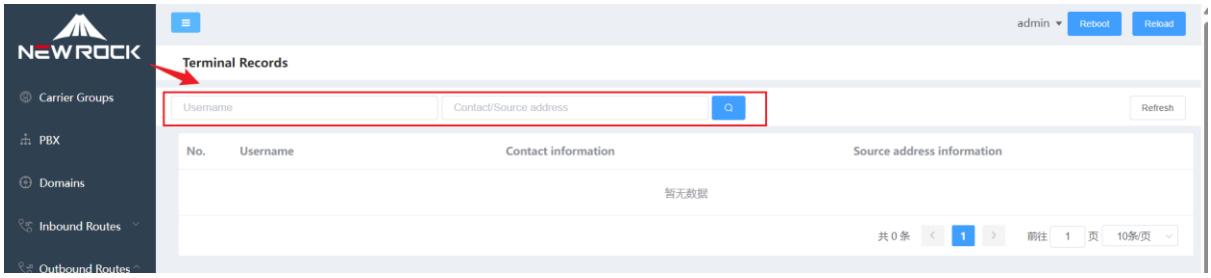


Figure36 Terminal Records

7.9 Call Record

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

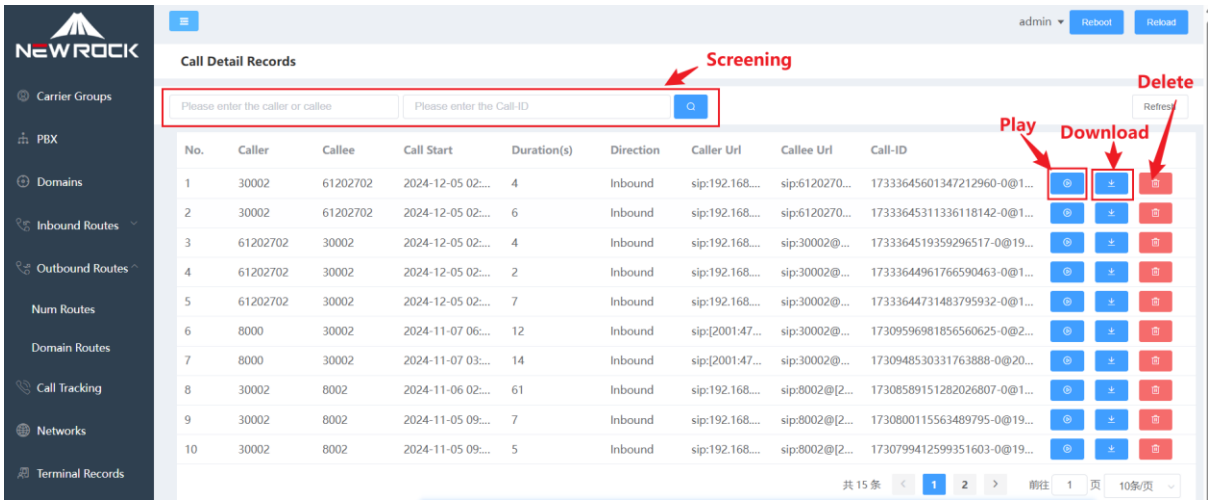


Figure37 Call Log

Table19 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.
Called address	The address of the receiving caller.
Call-ID	A unique identifier for each call that identifies a call session.

 Copyright© New Rock Technologies, Inc.

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.

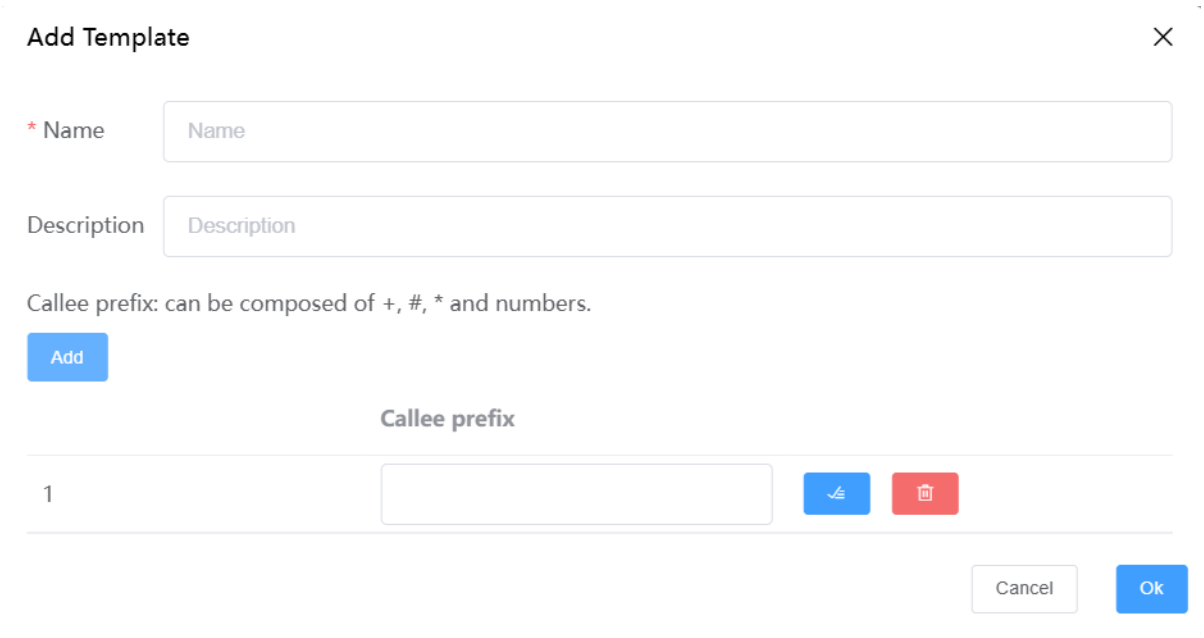


Figure38 New Template

Table20 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© New Rock Technologies, 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.

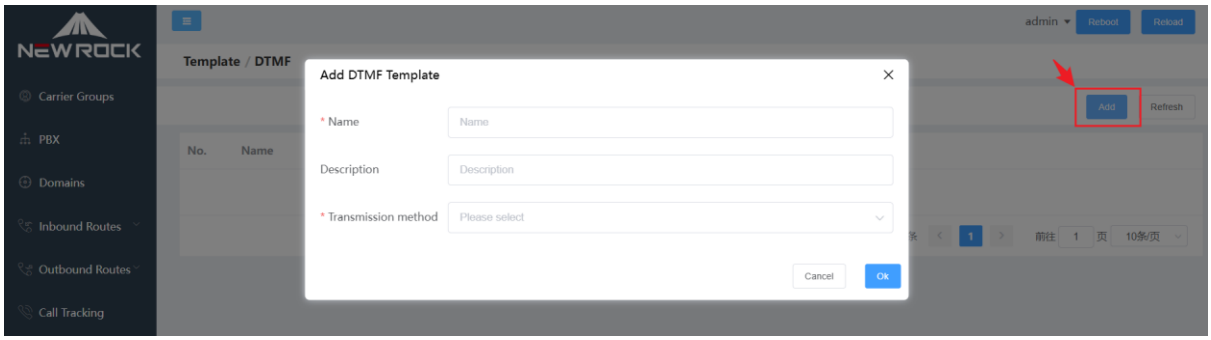


Figure39 New DTMF template

Table21 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.

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.

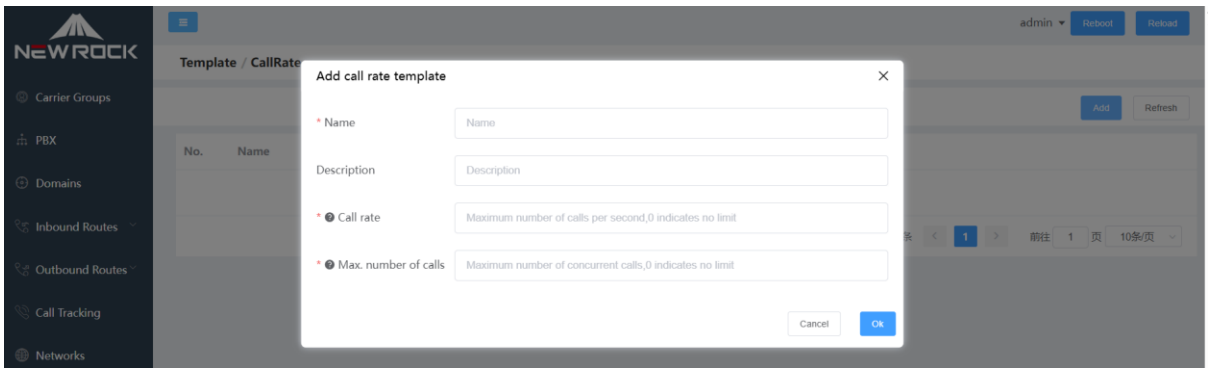


Figure40 Call Frequency Template

Table22 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.

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.

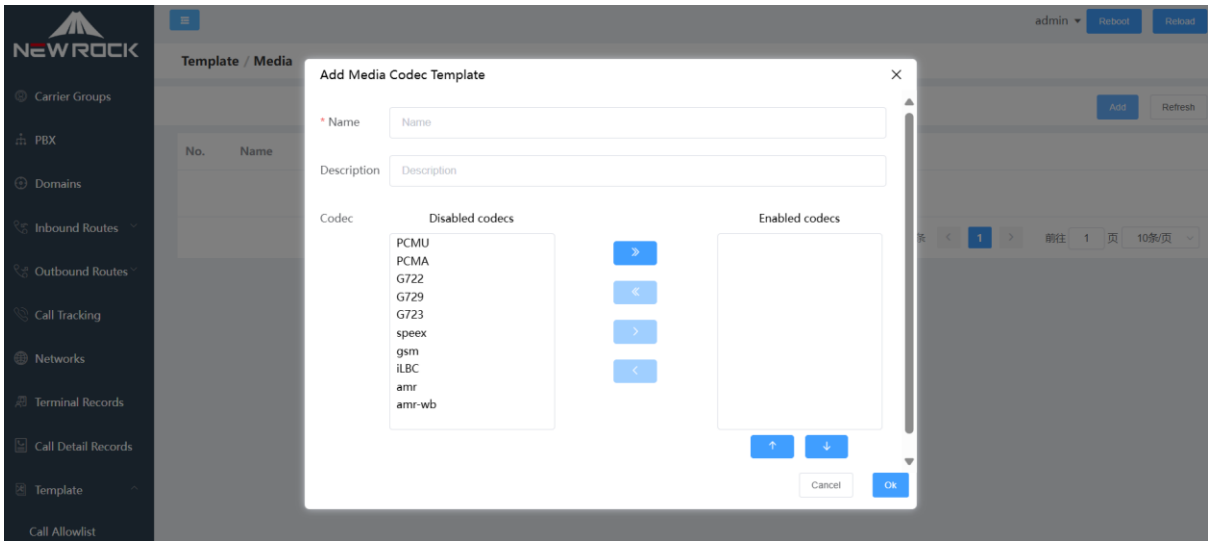


Figure41 Media Codec Template

Table23 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.

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.

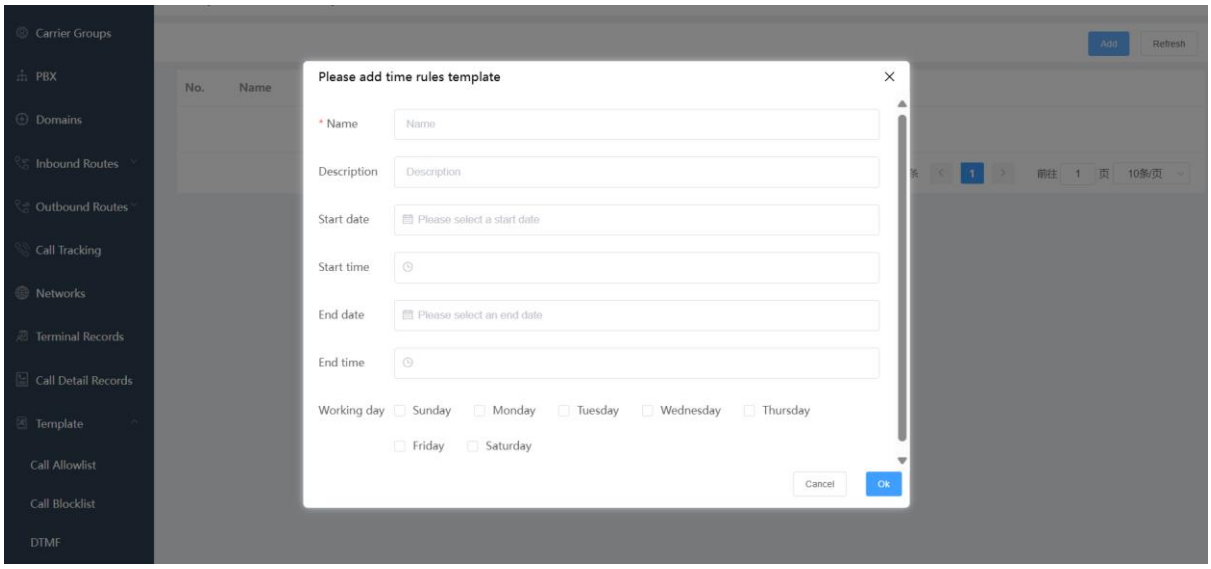


Figure42 Routing Effective Time Template

Table24 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.

7.10.6 Number Change Template

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

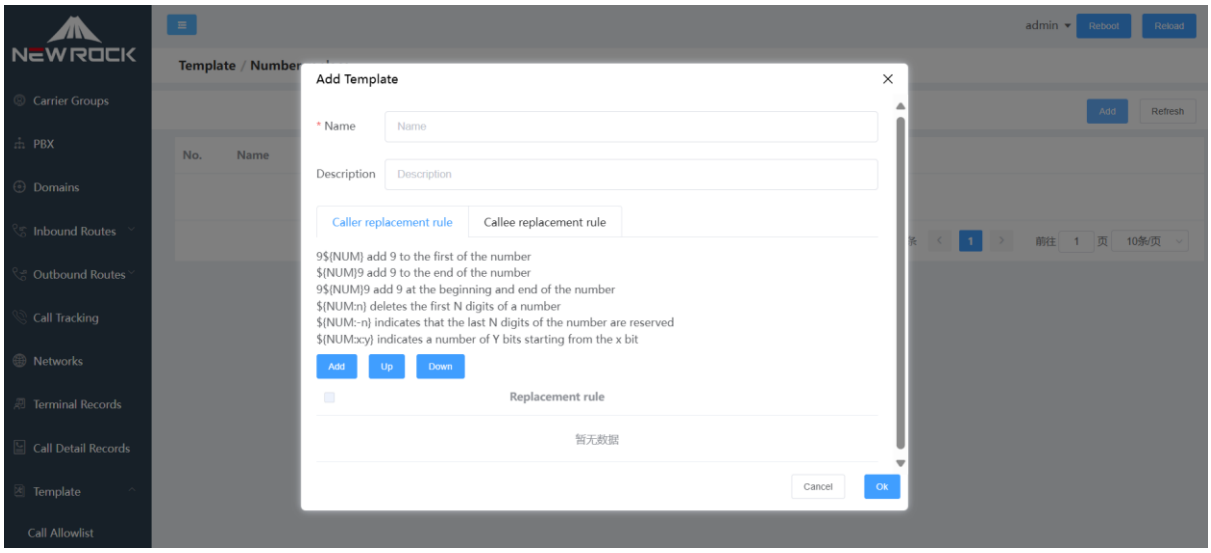


Figure43 Number Change Template

Table25 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

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.

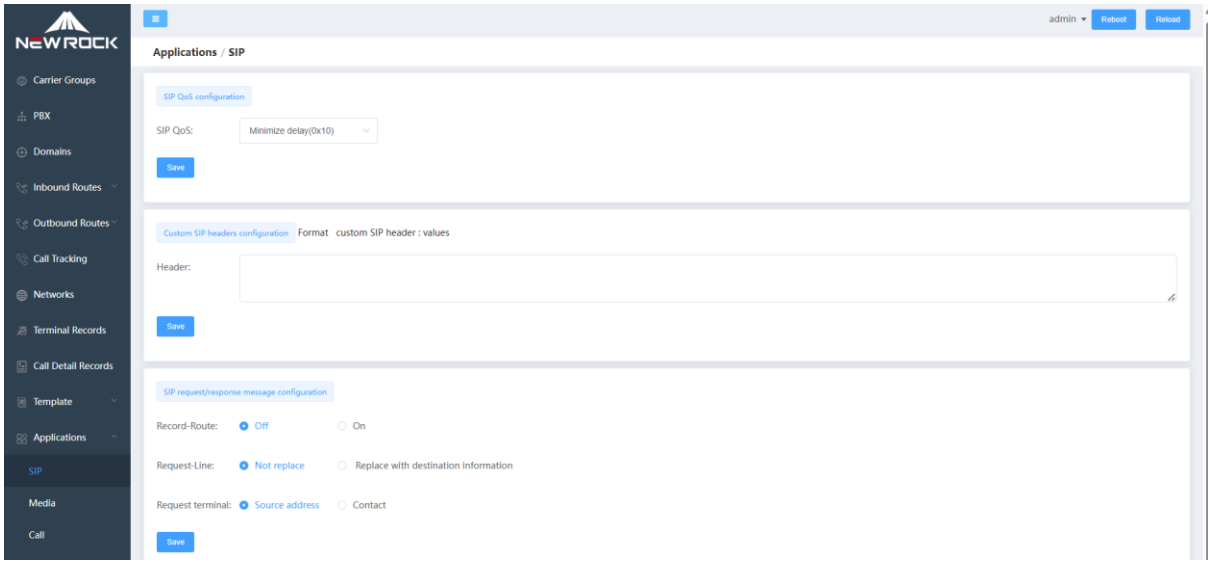


Figure44 SIP Configuration

Table26 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.
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

 Copyright© New Rock Technologies, Inc.

	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.

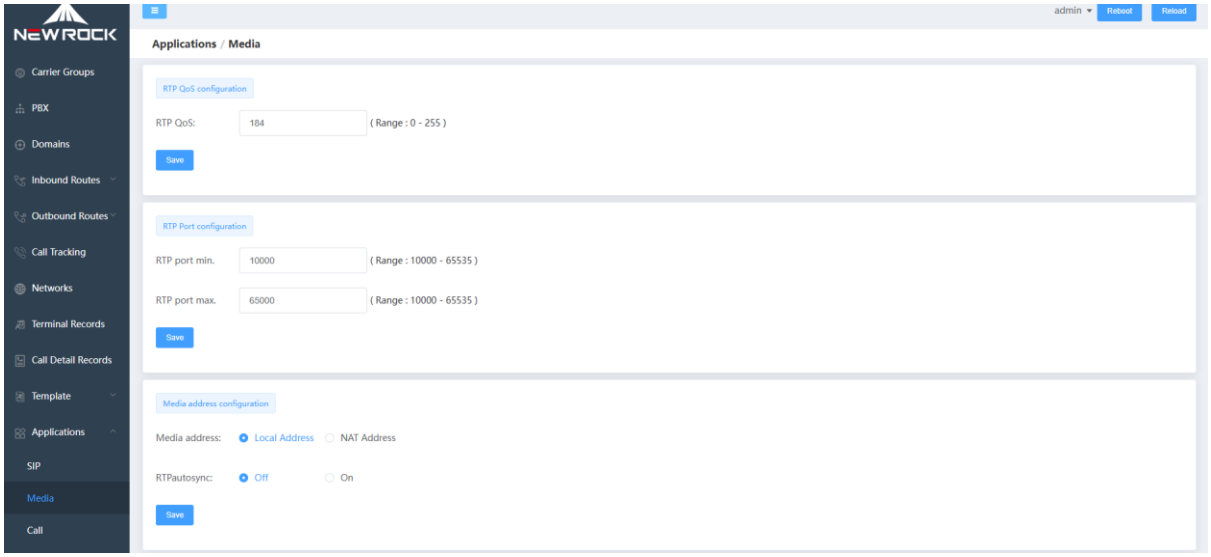


Figure45 Media Configuration

Table27 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.

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.

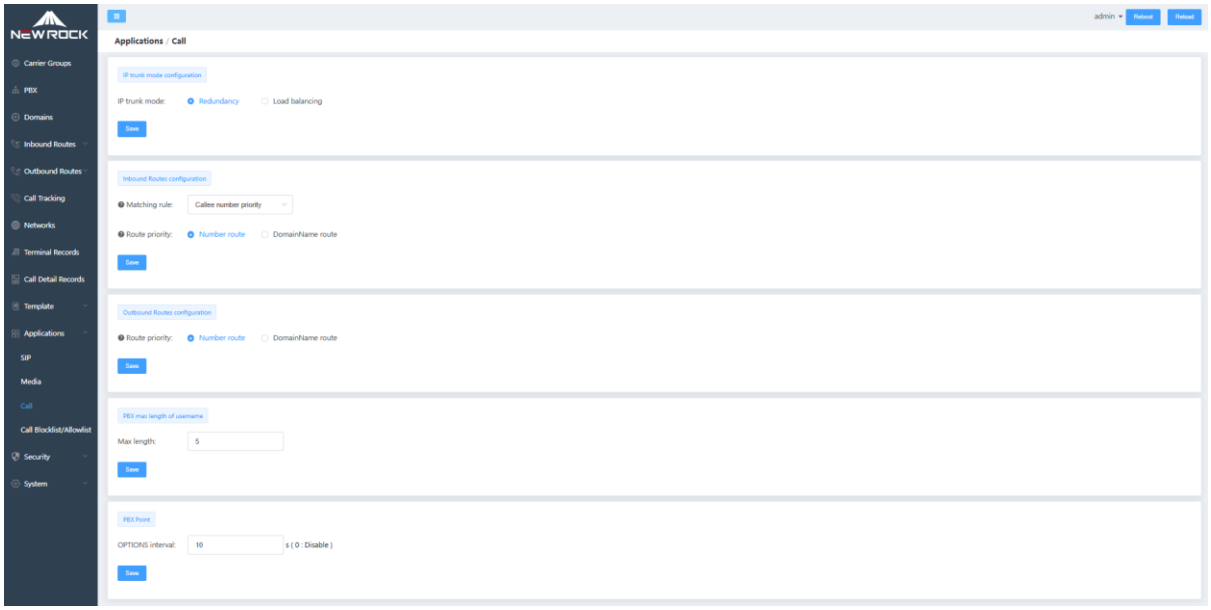


Figure46 Call Configuration

Table28 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 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.
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.

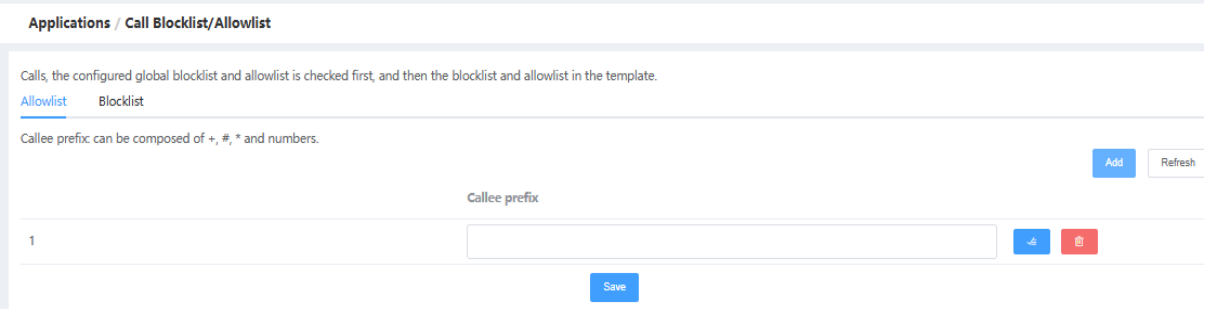


Figure47 Call Black/White List

Table29 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.

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.

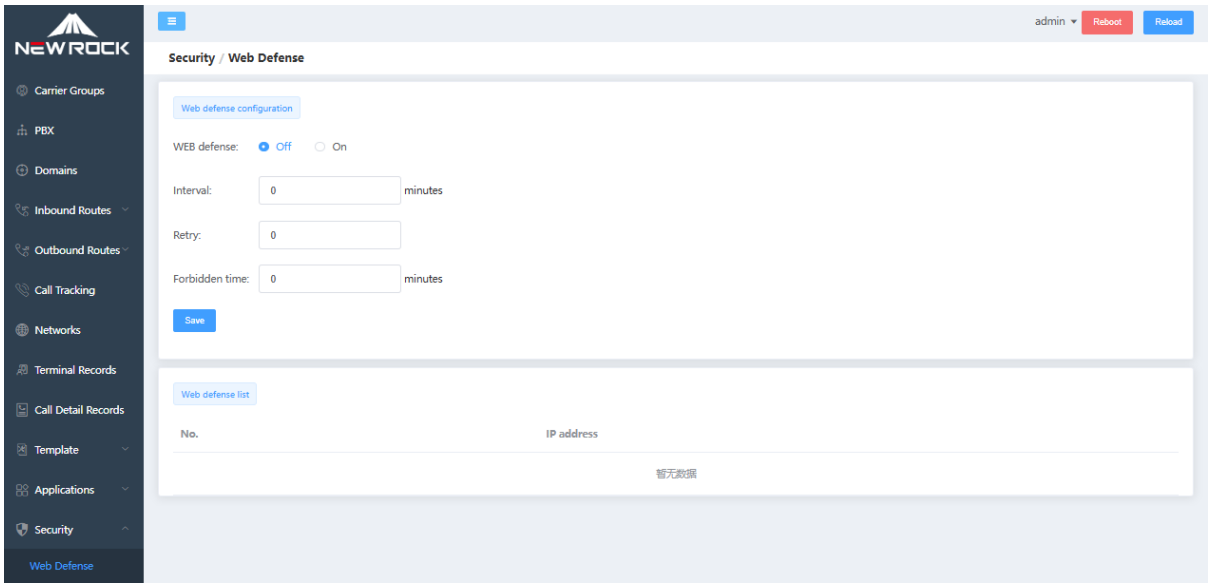


Figure48 WEB DEFENSE

Table30 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.

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.

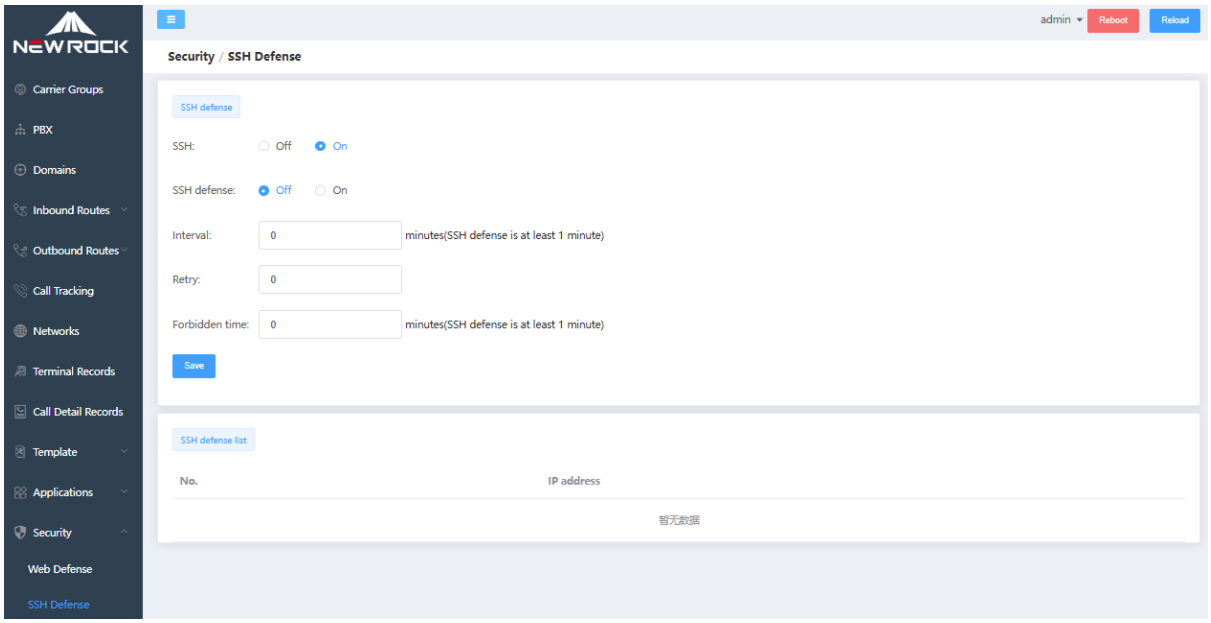


Figure49 SSH Defense

Table31 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.

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.

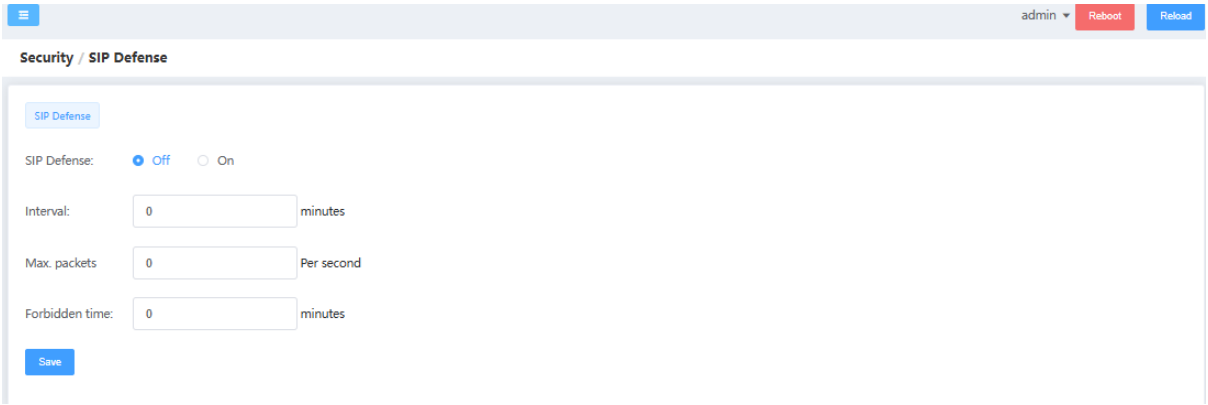


Figure50 SIP Defense

Table32 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© New Rock Technologies, 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.

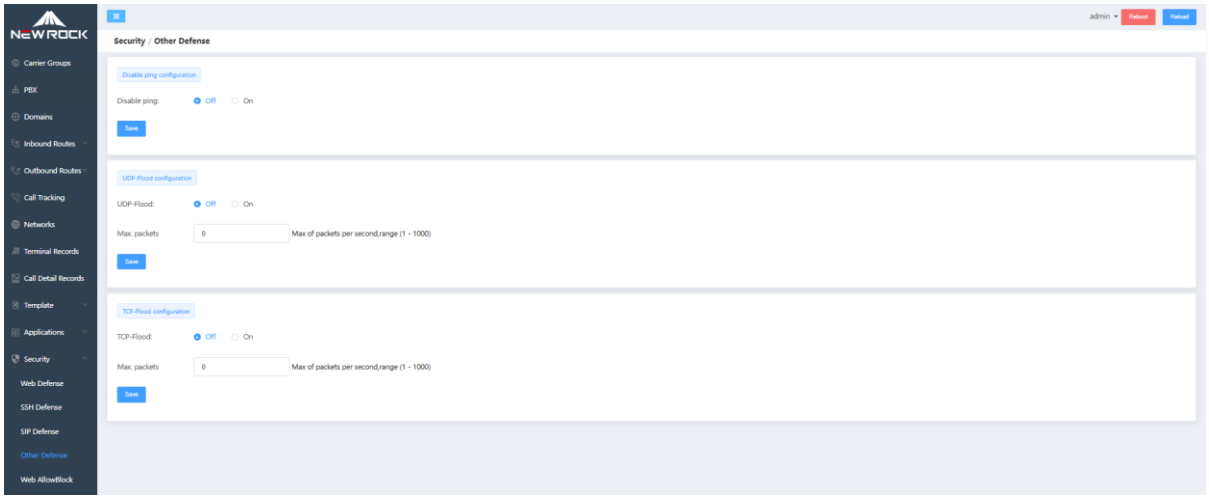


Figure51 Other defenses

Table33 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.

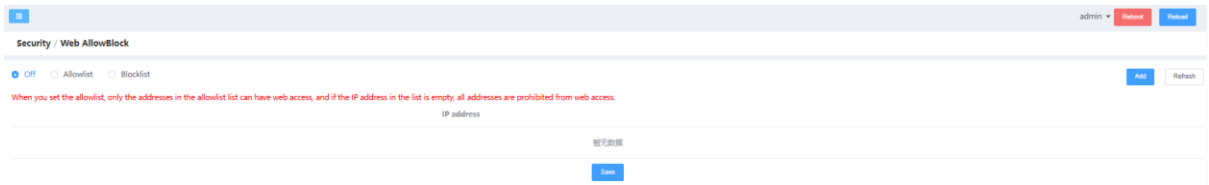


Figure52 Accessing the Black and White List

Table34 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.

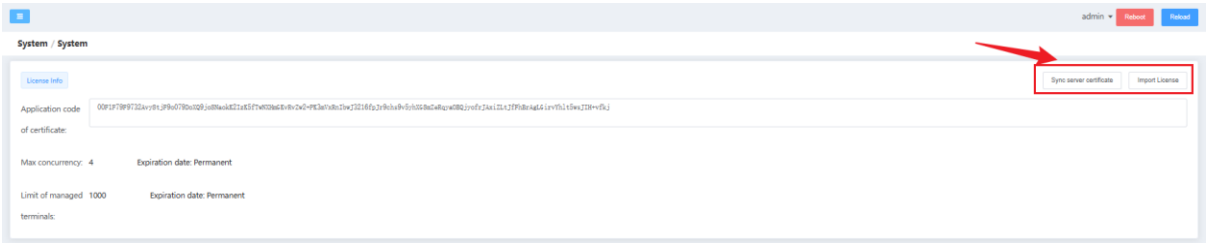


Figure53 System Configuration

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.

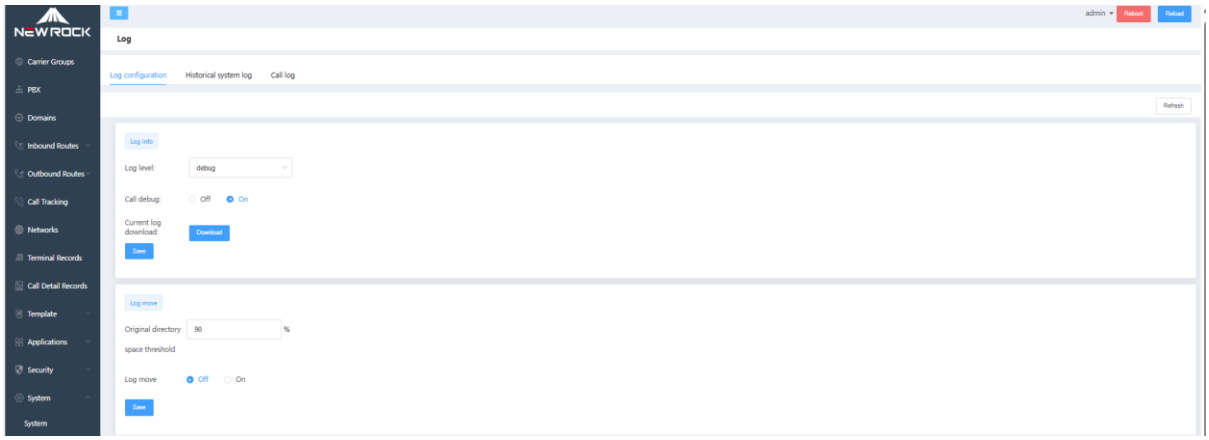


Figure54 Log Management

Table35 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.

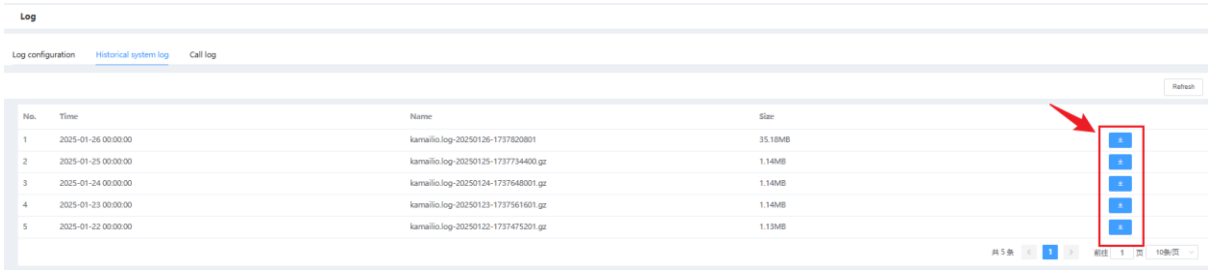


Figure 55 Historical System Log/Call Log

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 prevent data loss or system failure.

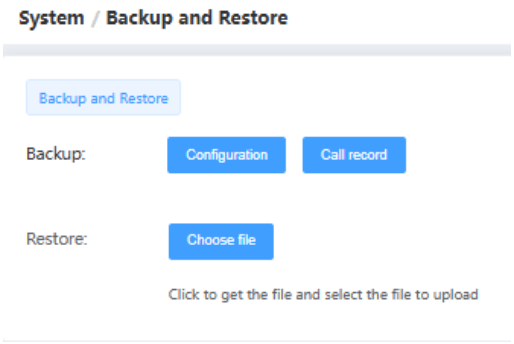


Figure56 Backup and Recovery

 Copyright© New Rock Technologies, Inc.

Table36 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.

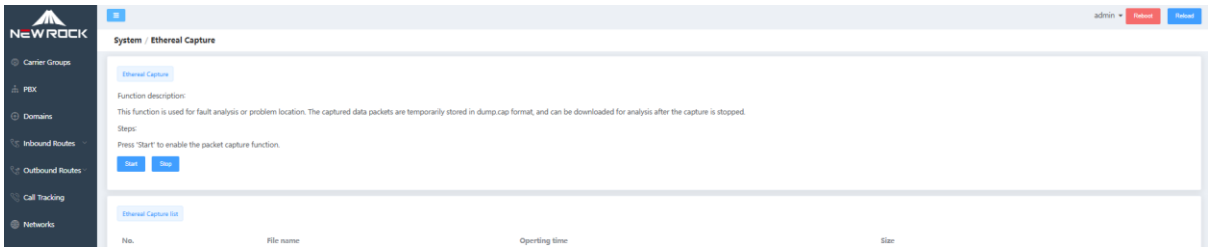


Figure57 Data Grab Bag

7.13.5 Operation Log

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

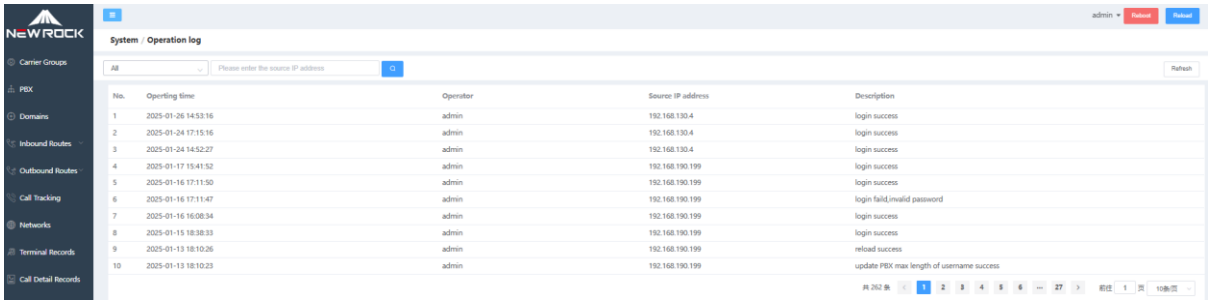


Figure58 Operation Log

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.



Figure59 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.

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© New Rock Technologies, 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© New Rock Technologies, 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© New Rock Technologies, Inc.