SX100 Session Border Controller
Product Specifications

CONTENTS

1 About This Document

The purpose of this document is to provide administrators who use and manage the SX100 Session Border Controller with comprehensive product specifications. It covers the technical parameters, functional features and performance specifications of the SX100. The information in this document is designed specifically for SX100 devices.

Explanation

Please read this document carefully and keep it in a safe place for future reference. Follow the recommendations in this document to ensure that you are able to manage and maintain your equipment efficiently. By following the guidance of this document, you will be able to fully utilize the performance of the SX100 Session Border Controller and ensure the security of your system.

1.1 Document Information

This section provides information from the SX100 Session Border Controller Product Specifications.

- Overview of Document Contents
- Versioning
- Symbol
- Revision of Information

1.1.1 Overview of Document Contents

Topic	Content Overview	Reader
Preface	Provides an overview of the purpose and important information about the SX100 Session Border Controller.	new users, system administrators
Product Overview	Provides basic information about the SX100, its product positioning, its market objectives, and the types of businesses for	all readers

	which it is suitable.	
Functions and Applications	System administrators, technical support team.	system administrators, technical support team
Performance Parameters	Lists the specific performance parameters and values of the SX100 Session Border Controller, demonstrating the processing power of the device.	system administrators, technical support team
Hardware Specifications	Details the hardware specifications of the SX100, including the basic hardware configuration, interface descriptions, and physical characteristics of the device.	system administrators, technical support team
Management and Monitoring	Introduces the SX100's management and monitoring tools, as well as remote management functions and how to use them.	system administrators, technical support team
Glossary	Provides a detailed explanation of technical terms and abbreviations used in this document.	system administrators, technical support team

1.1.2 Symbol

Icon	Description
Explanation	Text that serves as an explanation and adds details to the main body of the text.
Attention	Note text that reminds the user of important actions or to protect against potential threats.
Alert	Alert-type text that indicates a potential risk that could result in damage if not avoided.

1.1.3 Revision of Information

Document Version	Software Version	Date	Revision
V1.0.0	V1.1.9	August 2024	SX100 Session Border Controller V1.1.9 released

2 About New Rock Technologies

New Rock Technologies, Inc. is a leading company in digital solutions for smart communications and cloud services. We have devoted ourselves to the continuous combination of production and research in the field of converged communications, and our business has spread to nearly 100 countries around the world. Our products and technologies have been widely recognized and certified both domestically and internationally, and we have been awarded a total of more than a hundred of various corporate honors, qualification certificates, and product certifications both domestically and internationally.

2.1 Contact Us

Technical Support

For technical support, please contact your equipment seller or call us directly at 4007779719.

Web Contact

Visit the webpage of New Rock Technologies, Inc. at https://en.newrocktech.com/Login/index.html

- Register for support portal access.
- Get the latest news and announcements of the company.
- Realize online consulting service through webpage and provide instant communication function.

Documentation Information

- Go to the Documentation Center on the web page at https://en.newrocktech.com/DocumentCenter/index.html
- Check product descriptions and information materials.
- To ensure the security and accuracy of the information, please log in to your account before downloading product technical documentation and other related information. Only logged in users can download these documents.
- If you do not have an account, please register or contact technical support to obtain access.

Shanghai headquarters of New Rock Technologies, Inc.

Address: Block B, 5/F, Building 1, Caohejing Juxin Park, No.188 Pingfu Road, Xuhui District, Shanghai, China

Zip code: 200231

Tel: +86 021-61202700

E-mail: support@newrocktech.com

3 SX100 Session Border Controller Product Specifications

Performance and reliability are key factors when selecting and deploying enterprise communications equipment. SX100 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 device supports concurrent multi-user sessions, providing high-quality voice and video communications. By utilizing advanced encryption and security measures, the SX100 ensures the confidentiality and integrity of communications. In addition, a user-friendly management interface simplifies daily operation and maintenance.

Figure 1: SX100 Front View

Figure 2: SX100 Back View

3.1 Product Overview

SX100 Session Border Controller is a high-performance network device for small and medium-sized business users launched by New Rock Technologies, Inc. It provides high-quality session security data protection, offers communication security for enterprises, and addresses the problems brought by the evolution of enterprise voice networks, such as mobile office, branch interconnection, and multi-network integration.

3.1.1 Product Positioning and Market Objectives

Designed for small and medium-sized businesses, the SX100 Session Border Controller provides a high-performance and high-reliability communications solution. By supporting concurrent multi-user sessions and high-quality voice and video communications, the SX100 meets the needs of enterprises for mobile offices, branch interconnections and multi-network integration the SX100 meets the needs of enterprises for mobile offices, branch interconnections and multi-network integration. Its market positioning is to provide a secure, stable and easy-to-manage communication platform for small and medium-sized enterprises to ensure efficient internal and external communication.

3.2 Functions and Applications

This section details the functions of the SX100 Session Border Controller and its applicability in different application scenarios. The SX100 provides a reliable communications 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 administration and maintenance.

3.2.1 Functional Features

It mainly describes the capabilities and features of the device, including protocol support, security features, management capabilities, and so on.

- **Supports Dual-Machine (High Availability) HA Deployment**: Improves system availability by ensuring that if one device fails, the other seamlessly takes over, maintaining continuous system operation.
- **Standard Session Initiation Protocol (SIP) and Flexible Routing Rules**: The SX100 is perfectly compatible with IMS systems and supports flexible routing rule settings to adapt to different network environments and application scenarios.
- **User Support:** The SX100 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 Encoding Standards**: The device is compatible with a wide range of voice and video encoding 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, to ensure that it works 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, proxy registration, and trunk docking to facilitate 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 the Transport Layer Security (TLS) protocol, as well as support for Secure Real-Time Transport Protocol (SRTP) and Datagram Transport Layer Security (DTLS-SRTP) encrypted sessions to provide 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 Mechanisms**: Supports whitelist and blacklist management, topology hiding, attack defense for Denial-of-Service (DoS) and Distributed Denial of Service (DDoS) and provides voice firewall function to protect 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**: Supports call recording function, which is 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 Flood 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 (UDP/TCP), Real-Time Transport Protocol/Real-Time Transport Control Protocol (RTP/RTCP), Message Session Relay Protocol (MSRP), Transport Layer Security Protocol/Secure Real-Time Transport Protocol (TLS/SRTP), Session Initiation Protocol/Multimedia Subsystem over IP (SIP/IMS), Hypertext Transfer Protocol/Secure Hypertext Transfer Protocol (HTTP/HTTPS), Network Time Protocol/Simple Network Time Protocol (NTP/SNTP) with high compatibility.
- **Comprehensive Function Support**: Not only provides the interfacing solution for Session Initiation Protocol (SIP) and IP Multimedia Subsystem (IMS), but also supports

the functions of the standard SBC (Session Border Controller), 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, and call frequency limitation
- **Protocol Compatibility and Interoperability**: The SX100 session border controller is compatible with the mainstream signaling and media protocols on the market, eliminating differences between different manufacturers, solutions, and networks and helping enterprises achieve unified communications.
- **NGN and IMS Protocol Conversion**: The SX100 Session Border Controller (SBC) supports protocol conversion between Next Generation Network (NGN) and IP Multimedia Subsystem (IMS) systems. NGN is a next-generation network that handles the interconnection between traditional telephone networks (PSTN) and IP networks, and mainly manages the processing, forwarding, and conversion of media streams, enabling the transmission of voice, data, and other services between different networks. The IMS system, on the other hand, is an architectural framework that provides IP-based multimedia services such as voice, video calling and instant messages. With SX100 devices, efficient conversion of different signaling protocols (e.g., SIP, H.323) and media protocols between NGN and IMS can be achieved, 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**: SX100 devices support the proxy registration and forwarding registration functions of 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 B2BUA function, which acts as an intermediary between two SIP sessions, processes and modifies SIP messages to realize 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.

3.2.2 Functional Modules

The SX100 Session Border Controller provides a flexible and efficient communications solution for small and medium-sized businesses through its advanced functional modules. The following section details the specific functions of key modules such as call handling, security and management.

3.2.2.1 Call Processing Module

The Call Processing 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 setting of call paths to adapt to different network structures and needs.
- **Time Slot Policy**: Supports the selection of call routing according to the present time slot policy, realizing different call processing 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**: It supports heterogeneous network routing redundancy 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.

3.2.2.2 Security Module

The security module is responsible for ensuring data security and network protection during

the communication process. Its main functions include:

- **Access Control**: Use blacklisting and whitelisting mechanisms to control access to devices and network resources, ensuring that only authorized users have access.
- **Attack Defense**: Provides defense mechanisms to protect against a wide range of attack, which include:
  - **Denial of Service (DoS) Attack**: Prevents malicious users causing the system to run out of resources by sending a large number of requests.
  - **Distributed Denial of Service (DDoS) Attack**: Defense against attacks from multiple sources and protect systems from distributed attacks.
  - **UDP/TCP Flood Attack**: Prevents attacks that cause network congestion and resource exhaustion by sending large numbers of UDP or TCP packets.
- **SIP Attack Defense**: The policy-based Session Initiation Protocol (SIP) attack defense mechanism can detect and block malicious SIP traffic to protect communication security
- **Encrypted Sessions**: Provides a variety of encryption mechanisms to secure sessions, including:
  - **Transport Layer Security (TLS)**: Prevents data from being intercepted and tampered with during transmission by encrypting transport layer data.
  - **Secure Real-Time Transport Protocol (SRTP)**: Encrypts real-time voice and video data to ensure the security of real-time communication.
  - **Datagram Transport Layer Security Protocol DTLS-SRTP (DTLS)**: Combines DTLS and SRTP to provide enhanced real-time data encryption to ensure the security of datagram transmission.
- **Call Frequency Restriction**: Based on preset policies, limit the number of calls per unit of time to prevent misuse 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.

3.2.2.3 Management Module

The Management Module provides tools and functions that simplify and optimize

equipment management and maintenance. Its key features include:

- **Web-based Management Interface**: Provides a Web-based management interface, supporting 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 Secure Shell (SSH), 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 recover to the previous configuration status 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 function allows administrators to capture and analyze network data packets. This feature is useful for troubleshooting network problems, analyzing traffic and 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 operating 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 about all call activities, including call time, duration, and parties involved.

3.3 Specifications

This section provides a detailed description of each of the SX100 Session Border Controller's specification parameters. The content includes the performance indicators of the equipment, network protocol support, transmission capabilities, quality of service control, and voice and video processing capabilities. This information provides a comprehensive understanding of the SX100's performance and application capabilities and provides a reference for configuration and deployment.

3.3.1 Performance Parameters

Performance Indicators	Value/Description
Call Concurrency	Maximum 120 (unencrypted) / 100 (encrypted) concurrent calls
Transcoding Concurrency	Maximum 70 channels of encoding and decoding conversion
Call Pers Second (CPS)	20 calls per second
Registered Users	Maximum 1000 registered users
Audio and Video Codecs	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 Type of Service (TOS), Differentiated Services (DiffServ)
Voice Gain Control	Fixed/dynamic voice gain control
Jitter Buffer	Support
Fax	G.711 pass-through fax, T.38 fax, compatible with class G3 fax machines, up to 33.6 kbps (pass-through)
Dual Tone Multi-Frequency Mode	RFC2833、SIP-INFO、INBAND
Network Protocol	IPv4/IPv6、SSH、HTTP/HTTPS、DNS、ARP、NTP/SNTP、ICMP
Transport Protocol	UDP/TCP、RTP/RTCP/MSRP、TLS/SRTP

Detailed list of specific performance indicators and values:

- **Call Concurrency**: Maximum 120 (unencrypted) / 100 (encrypted) concurrent calls
  - Indicates the maximum number of calls that the device can handle at the same time for both the unencrypted and encrypted case values.

- **Transcoding Concurrency**: Maximum 70 channels of encoding and decoding conversion
  - Indicates the maximum number of codec conversions that the device can perform at the same time, ensuring efficient conversion of multiple voice or video streams.
- **Call Pers Second (CPS)**: 20 calls per second
  - Indicates the number of call requests per second (CPS) that the device can handle, and the device's call handling capability under high load conditions.
- **Registered Users**: Maximum 1000 registered users
  - Indicates the maximum number of users the device can register.
- **Audio and Video Codecs**：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
  - Indicates the voice and video encoding standards supported by the device, ensuring that the device is compatible with different communication systems and devices and provides high-quality voice and video transmission.

Audio and Video Codecs Support List

Codec Types	Supported Codecs	Description
Audio Encoding and Decoding	G.711（A-Law / U-Law）	High fidelity voice, 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 broadband-limited networks.
	iLBC	Internet low-bandwidth codec for voice transmission in unstable network environments.
	G.722	Broadband audio codec for higher sound quality.
	G.722.1	Improved broadband audio codec for conference systems.
	G.722.2	Broadcast-quality voice codec for high-

		definition voice communications.
	AMR	Adaptive multi-rate codecs, commonly used in mobile communication systems
Video Encoding and Decoding	H.264	Widely used high-definition video codec for a variety of video communication applications.
	H.265	Higher compression efficiency video codec for ultra-high definition video transmission.

- **Quality of Service (QoS)**:

Overall concept of ensuring that specific data flows in a network are processed on a priority basis through technical methods.

- **802.1p/Q VLAN tagging**:
  - Indicates that by setting priority labels for network traffic, it ensures that important data packets (e.g., voice and video) are prioritized through the network, reducing delay and packet loss, and is used for priority management of network traffic to improve the efficiency of transmission of important data.
- **IP Type of Service (TOS)**:
  - The SX100 device supports IP Type of Service (TOS). By setting the TOS field, the network device can specify the priority and type of service for data packets to ensure that critical communication data packets are prioritized, thus improving network performance and quality of service. This mechanism is relatively simple and is suitable for basic priority marking.
- **Differentiated Services (DiffServ)**:
  - SX100 devices support DiffServ, which manages network traffic by marking data packets with a priority (DSCP field) to ensure that high-priority data, such as voice and video, is served first. DiffServ provides more flexible and fine-grained traffic management capabilities for prioritization control in large-scale and complex network environments.
- **Fixed/Dynamic Voice Gain Control**:

    - Indicates that the gain of the voice signal is adjusted to ensure that the proper volume is maintained during transmission and that the signal strength is automatically adjusted to improve voice quality.
  - **Jitter Buffer**：
    - Indicates the use of a buffer at the receiving end to absorb jitter in network transmissions, ensuring that voice data is continuous and smooth and reducing lags in calls.
- **Fax**: G.711 pass-through fax, T.38 fax, compatible with class G3 fax machines up to 33.6 kbps (pass-through)
  - Indicates the fax standards and compatibility supported by the device to ensure the reliability of fax communications.
- **Dual-Tone Multi-Frequency (DTMF)**：RFC2833、SIP-INFO、INBAND
  - Indicates the Dual-Tone Multi-Frequency (DTMF) signal transmission mode supported by the device for key signals.
- **Network Protocols**: IPv4/IPv6, SSH, HTTP/HTTPS, DNS, ARP, NTP/SNTP, ICMP
  - Indicates the network protocols supported by the device, ensuring that the device can operate in a variety of network environments.
- **Transport Protocols**: UDP/TCP, RTP/RTCP/MSRP, TLS/SRTP
  - Indicates the transport protocol supported by the device to ensure reliable data transmission and encryption protection.

3.3.2 Hardware Specifications

This section provides detailed hardware specifications for the SX100 session border controller. It covers the basic hardware configuration of the device, physical and mechanical specifications, and descriptions of front and back 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.

3.3.2.1 Basic specifications

Item	Specification	Description

CPU (Processor)	2.60GHz main frequency	High performance processor to ensure fast data processing and system response.
System Memory	8GB	Adequate memory capacity to support multitasking and stable operation.
System Storage	250GB	Large capacity storage for system data and logs.
Ethernet Port	6 x 10/100/1000Mbps Adaptive Ethernet ports	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×W×H)	430mm × 300mm × 45mm	The chassis size is suitable for a variety of installation environments.
Power Supply	100-240 volts, 50/60 Hz, 1A	Compatible with electrical standards in different regions of the world
Working Environment	Temperature： -15 ~ 60℃, Relative humidity: 10% - 90% (non-condensing)	Adapt to extreme working environment to ensure stable operation of equipment.
Storage Environment	Temperature： -40 ~ 70℃, Relative humidity: 5% - 90% (non-condensing)	Ensure that the equipment is kept undamaged for long periods of time.
Power Consumption	50W	The power consumption of a device under normal operating conditions.
Certification and Standards	CQC	International and national standards and certifications to which the equipment conforms.

3.3.2.2 Physical and Mechanical Specifications

Specification	Description
Weight	3.7kg

Interfaces	6 10/100/1000Mbps adaptive network ports; 2 USB ports (not enabled yet); 1 CONSOLE port (not enabled yet); 1 VGA port (not enabled yet)
Cooling System	2 fans
Power Supply	Standard power connector with switch
Power Connector	250V fuse only
Mounting Methods	Rack-mounted and tabletop

3.3.2.3 Front Panel Component Description

Port Name	Type	Description	Purpose
CONSOLE	RJ45	1 CONSOLE interface (not enabled yet)	This interface is currently not enabled and may be supported in the future through software updates or other ways to provide functionality.
USB	USB 3.0	2 USB ports (not enabled yet)	This interface is currently not enabled and may be supported in the future through software updates or other ways to provide functionality.
ETH0	RJ45	10/100/1000Mbps Adaptive Ethernet port	Connects to a LAN switch or router
ETH1	RJ45	10/100/1000Mbps Adaptive Ethernet port	Connects to a LAN switch or router
ETH2	RJ45	10/100/1000Mbps Adaptive Ethernet port	Connects to a LAN switch or router
ETH3	RJ45	10/100/1000Mbps Adaptive Ethernet port	Connects to a LAN switch or router
ETH4	RJ45	10/100/1000Mbps Adaptive Ethernet port	Connects to a LAN switch or router
ETH5	RJ45	10/100/1000Mbps Adaptive Ethernet port	Connects to a LAN switch or router
PWR Indicator	LED	Power indicator	Indicates the power status of the device

HDD Indicator	LED	Hard disk indicator	Indicates the operating status of the hard disk

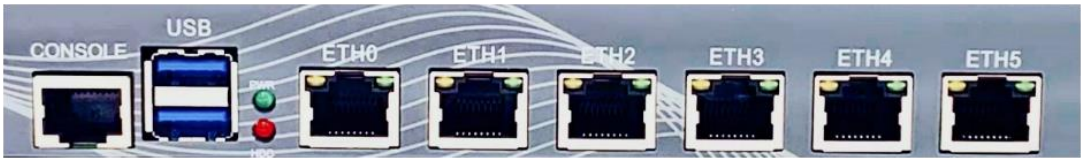

Figure 4: Front Panel Diagram

3.3.2.4 Back Panel Component Description

Port Name	Type	Description	Purpose
VGA	DB-15	VGA interface (not enabled yet)	This interface is currently not enabled and may be supported in the future through software updates or other ways to provide functionality.
POWER	IEC C14	Power connector with switch	Connection to the power supply to power the device
Fan	Built-in	Used to dissipate heat inside the device to keep the device temperature stable	Ensure device stability under high loads

Figure 5: Back Panel Diagram

3.4 Management and Monitoring

This section describes the SX100 Session Border Controller's management and monitoring tools, as well as the remote management features and their usage. These tools and functions provide administrators with an efficient way to manage devices, to ensure stable operation and quick troubleshooting

3.4.1 Management Tools

The SX100 Session Border Controller provides a variety of management and monitoring tools to meet the needs of different users:

- **CLI Commands**: Accessed via Secure Shell Protocol (SSH), providing advanced configuration and maintenance operations for scenarios requiring fine-grained control.
- **Web Interface**: Web-based management interface, supporting 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.

3.4.2 Remote Management

The SX100 device supports remote management via a command line interface (CLI) and background services, enabling administrators to configure and maintain the device 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 function enable/disable on the device without being on site, improving management efficiently.
- **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 operating status, configuration change records and call activities for troubleshooting and performance optimization.

3.5 Glossary of Terms

To help the user better understand the technical terms and abbreviations used in this document, this section provides a detailed explanation of the terminology.

Letter	Term	Explanation
A	**AMR (Adaptive Multi-Rate)**	Adaptive multi-rate, an audio codec standard used for speech compression.
A	**API (Application Programming Interface)**	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, device configuration and management through the command line.
C	**CQC (China Quality Certification Center)**	China Quality Certification, the official quality certification organization in China.
C	**CDR (Call Detail Recording)**	CDR is a system that records detailed information (e.g., call duration, start and end time, participant number) about each call activity, which is used to analyze call data and calculate charges.
D	**DiffServ (Differentiated Services)**	Differentiated Services, manages network flows by prioritizing packets.
D	**DDoS (Distributed Denial of Service Attack)**	Distributed Denial of Service, a type of cyber-attack that attacks a target system from 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 combining DTLS and SRTP.
D	**DTMF (Dual-Tone Multi-Frequency Mode)**	Dual-Tone Multi-Frequency, used for the transmission of key signals, commonly used in telephone dialing and communication systems.
F	**FSP (Field Security Protocol)**	FSP is a security protocol used to authenticate devices and ensure secure communications.
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, improves the availability of the system through dual-machine hot backups to ensure continuous operation of the system.
H	**HTTP / HTTPS (Hypertext Transfer Protocol)**	Hypertext Transfer Protocol / Hypertext Transfer Protocol Secure, used for data transfer over the web, HTTPS provides encrypted secure transmission.
I	**ICMP (Internet Control Message Protocol)**	Used to transfer control information in IP networks, often used to diagnose and manage networks.
I	**IMS (IP Multimedia Subsystem)**	IP Multimedia Subsystem, is an IP-based multimedia service architecture that supports voice, video and multimedia communications.
I	**iLBC (internet Low Bitrate Codec for Voice)**	internet Low Bitrate Codec, a codec for voice communication in low broadband environments.
J	**Jitter Buffer**	Buffer used at the receiving end to absorb jitter in network transmissions to ensure smooth and continuous voice data.
L	**LDAP (Lightweight Directory Access Protocol)**	LDAP helps computers find and manage people or device information such as e-mail addresses or printers on the network, and is commonly used for user and resource management within organizations.
M	**MSRP (Message Session Relay Protocol)**	Message Session Relay Protocol, a protocol used for instant message transmission.
N	**NGN (Next Generation Network)**	Next Generation Network, is a packet-switching based network architecture designed to provide a variety of telecommunications services (including voice, data and multimedia services).
N	**NAT (Network Address Transfermation)**	network address transformation, used to transfer 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, used for network time synchronization to ensure that all devices have the same time.

R	**RTP (Real-Time Transfer Protocol) / RTCP (Real-Time Control Protocol)**	Real-Time Transfer 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 operates with resources on the network via standard HTTP methods (e.g., GET, POST, PUT, DELETE), often used in the design of APIs to support representational state transfer of resources.
S	**SBC (Session Border Controller)**	Session Border Controller, provides call control and session management functions 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 Transfer Protocol)**	Secure Real-Time Transfer Protocol, used to encrypt real-time voice and video data to ensure secure communications.
S	**SSH (Secure Shell Protocol)**	Secure Shell, encrypted command line interface management for secure remote access.
S	**SSL (Security Layer Protocol)**	SSL is a security protocol used to establish an encrypted connection over a computer network to ensure the security of data as it is transferred 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 ensure that packets are transmitted accurately and without error through an acknowledgement and retransmission mechanism, and is suitable for applications that require high reliability, such as e-mail and file transfers.
U	**UDP (User Datagram Protocol)**	UDP is a fast network transfer 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 a network into logical segments for network isolation and traffic management.
V	**VGA (Video Graphics Array)**	Video Graphics Array, an interface for display output.

Copyright Statement