SBC8000 Session Border Controller

User Manual

Shenzhen Dinstar Co., Ltd.
Address: Floor 18, Building 7A, Vanke Cloud City Phase 1, Xingke 1st Street, Xili Sub-district, Nanshan District, Shenzhen.
Postal Code: 518052
Telephone: +86 755 61919966
Fax: +86 755 26456659
Emails: sales@dinstar.com, support@dinstar.com
Website: www.dinstar.com

Preface

Welcome

Thanks for choosing **SBC8000 Session Border Controller**! We hope you will make full use of this rich-feature device. Contact us at 0086-755-26456110/112 if you need any technical support.

About This Manual

In order to help you understand and use SBC8000 Session Border Controller, we have written the user manual of this product, which mainly introduces the application scenarios, functional features, installation methods, network connection and Web configuration. Please read the manual carefully before installing it.

Intended Audience

This manual is primarily aimed at the following persons:

- Users
- Engineers who install, configure and maintain SBC8000 System

Revision Record

Document Name	SBC8000 Session Border Controller User Manual
Document Version	V1.0
Author	Ellie Zhang
Date	2022/12/25
Firmware Version	1/2.94.1.1

Conventions

System mentioned in this document refers to the SBC8000 Session Border Controller. Those key words specially noted in the document are the contents that users need to pay attention to.

1 Introduction of SBC8000

1.1 Overview

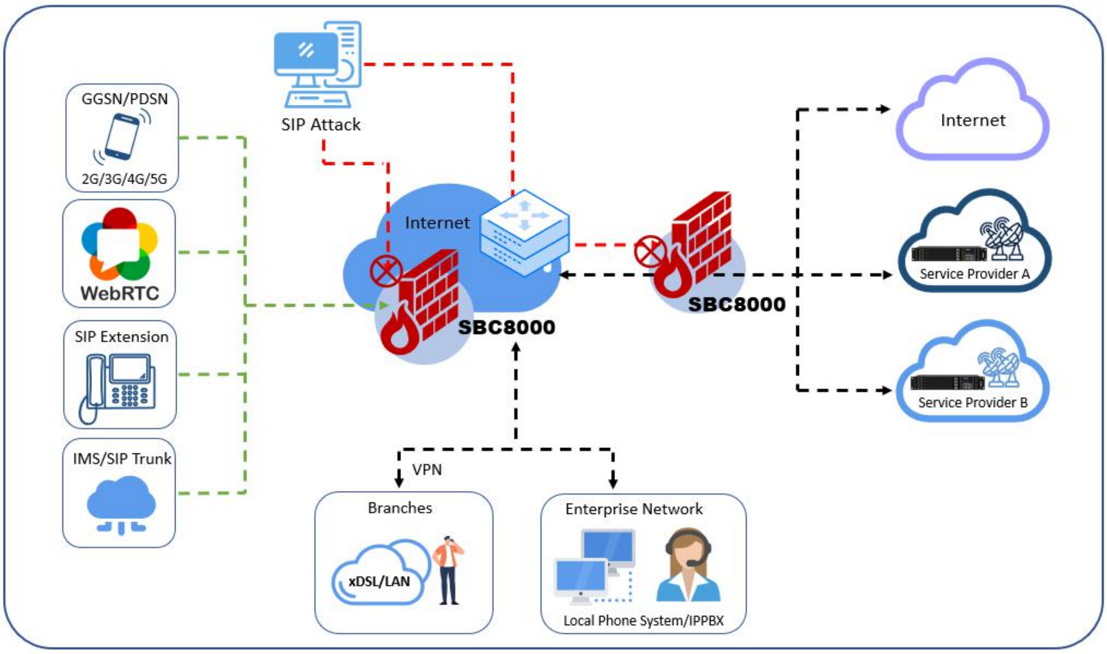
With the rapid development of unified communication and All-IP network, more and more enterprises begin to construct their own IP-based communication system by using IP-PBX and software to improve communication within organization efficiency and security. However, they need to ensure NAT traversal for IP multimedia services and the safe access of users. Dinstar SBC8000 (Session Border Controller) can help enterprises to solve the above mentioned problem.

Dinstar SBC8000 (Session Border Controller) solution can solve two major problems for enterprise IP communication system at low cost: terminal access security and NAT traversal for IP multimedia services.

SBC8000 is built without the limitation of embedded hardware and can be installed on various server platforms: x86, ARM, Kunpeng or Huawei cloud/Ali cloud, etc., which greatly improves its performance and facilitates deployment migration. It supports up to 100,000 SIP registrations, 10,000 concurrent sessions and 5,000 voice media transcoding processing, and supports SIP over TLS, SRTP encrypted sessions. In addition to traditional telecom codecs, media processing also supports wireless and Internet codec conversions such as AMR, OPUS and iLBC.

1.2 Application Scenario

Figure 1-2-1 Application Scenario of SBC8000



1.3 Functions and Features

1.3.1 Key Features

- Support up to 10,000(Max) concurrent call sessions, 5,000 media transcoding and 100,000(Max)SIP registrations
- Support physical server, virtual machine and public cloud deployments
- Support intelligent bandwidth limit and dynamic blacklist
- Support cross-network and NAT traversal and high availability(HA)
- Support SIP over TLS, SRTP
- Compatible with different codecs: G.711A/U, G.723.1,G.729A/B, iLBC, AMR, OPUS
- Support flexible call routing
- Perfectly compatible with IMS network

- Provide VoIP firewall, anti-attacks and core networkprotection
- Support call recording

1.3.2 Capabilities

- Concurrent Calls

  Supports 10,000 SIP sessions at maximum

- Transcoding

  Supports 5,000 transcoding calls

- CPS for call

  800 calls per second at maximum

- Registrations

  Up to 100,000 SIP registrations

- CPS for Registration

  800 Registration per second

1.3.3 VoIP

- SIP 2.0 Compliant, UDP, TCP, TLS
- SIP Trunk (Peer to peer)
- SIP Trunk (Access)
- SIP Proxy Registrations: Up to 3,000
- B2BUA (Back-to-Back User Agent)
- SIP Request Rate Limiting
- SIP Registration Rate Limiting
- SIP Registration Scan Attack Detection
- SIP Call Scan Attack Detection

- SIP Header Manipulation
- SIP Malformed Packet Protection
- Multiple Soft-switches Supported
- QoS (ToS, DSCP)
- NAT Traversal

1.3.4 Media Capabilities

- Codecs：G.711a/μ, G.723,G.729A/B, iLBC, G.726, AMR,OPUS
- Silence Suppression
- Voice Activity Detection(VAD)
- Comfort Noise Generator(CNG)
- Echo Cancellation: G.168 with up to 128ms
- RTP/RTCP
- Voice Interrupt Protection
- Adaptive Dynamic Buffer
- Adjustable Gain Control
- Automatic Gain Control (AGC)
- FAX: T.38, Pass-through
- DTMF: RFC2833/Signal/Inband

1.3.5 Security

- Prevention of DoS and DDoS Attacks
- Control of Access Policies
- Policy-based Anti-attacks
- Message format detection and processing

- UDP-Flood Anti-attacks
- TCP-Flood Anti-attacks
- Call Security with TLS/SRTP
- White List & Black List
- Access Control List
- Built-in VoIP Firewall

1.3.6 Call Control

- Dynamic Load Balancing and Call Routing
- Flexible Routing Engine
- Routing Based on Caller/Called Prefixes
- Regular Express
- Call Routing Base on Time Profile
- Call Routing Base on SIP URI
- Call Routing Base on SIP Method
- Caller/ Called Number Manipulation

1.3.7 Maintenance

- Web-bases GUI for Configurations
- Configuration Restore/Backup
- HTTP Firmware Upgrade
- CDR Report and Export
- Ping and Tracert
- Network Capture
- System log

- Statistics and Reports
- NTP
- SNMP
- TR069
- Remote Web and Telnet

2 Installation

2.1 Server Requirements

2.1.1 Basic system requirements

If you want to support up to **1,000** concurrent call sessions and **10,000** SIP registrations, the following or higher configurations are recommended.

Name	Requirement
CPU	Intel(R) Core(TM)i7-1070F CPU @ 2.90 GHz
Memory	8G
Hard Disk	1TB
Ethernet port	Gigabit Ethernet ports, 2 or more

2.1.2 Medium size system requirements

If you want to support up to **5,000** concurrent call sessions and **50,000** SIP registrations, the following or higher configurations are recommended.

Name	Requirement
CPU	Intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz
Memory	16G
Hard Disk	1TB
Ethernet port	Gigabit Ethernet ports, 2 or more

2.1.3 Large size system requirements

If you want to support up to **10,000** concurrent call sessions and **100,000** SIP registrations, the following or higher configurations are recommended.

Name	Requirement
CPU	Intel(R) Xeon(R) Gold 5218 CPU @ 2.30GHz
Memory	32G
Hard Disk	1TB
Ethernet port	Gigabit Ethernet ports, 2 or more

2.2 Operating System

The server needs to be pre-installed with the Linux OS. The specific version requirements are as follows:

- SUSE Linux Version 12 SP5 and higher
- Ubuntu Linux Version 21.04 and higher
- Centos Linux Version 7 and higher

The following are additional configuration requirements.

- Network Configuration

  The software installation package and subsequent license files need to be transferred over the network, so users also need to support mount or other file transfer methods, and open the relevant ports. The default https port of SBC8000 is 1081.

- User Permission

  In general, SBC8000 does not run with the Root User. So, you need to create a user for SBC8000. For example, you can create a user named SBC8000, which belongs to the Users Group.

2.3 Access Tools

- Web Browser

  Google Chrome is a very popular web browser designed to be fast and lightweight. It was developed by Google in order to make surfing the web easier even as technology changes.

2.4 SBC8000 Installation

Due to the difference of operating systems, there is a little difference in the installation of SBC8000. Please contact technical support for SBC8000 installation, DSP license and license application.

3 Configurations on Web Interface

3.1 Log in Web Interface

Software-based SBC8000 does not have a default IP. The default user name and password for the first installation are admin and admin@123#. The login IP is the IP address of the network port set during the installation of SBC8000 (https:// IP Address of Network Port). You can log in to the system by entering the default user name and password and random security verification code.

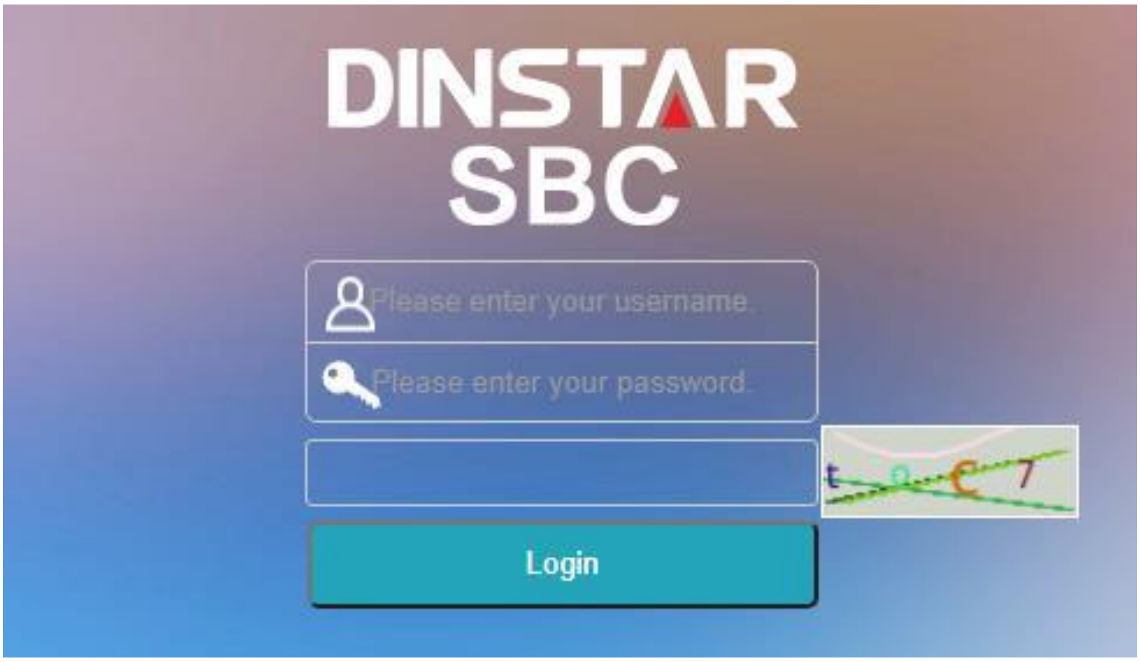


Figure 3-1-1 Login GUI

Note:

> The SBC8000 does not support http connection, user must use https connection to log in to the web page of the system.

For security consideration, when you logs in the system, it is enforced that you should modify the username and password on the **System** -> **Users** -> **Password** page

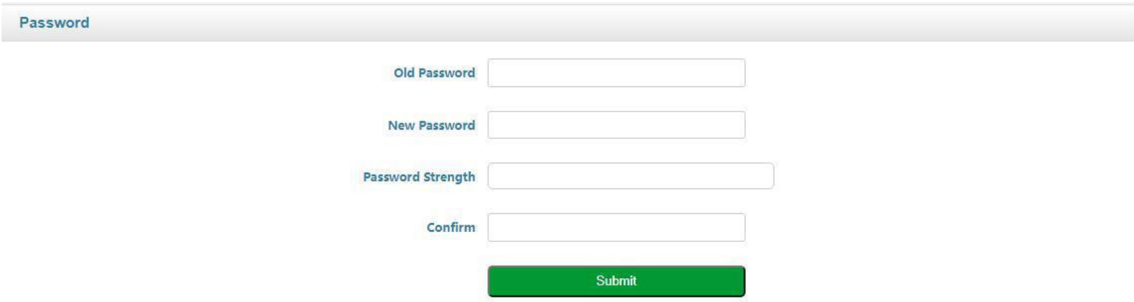


Figure 3-1-2 Modify Password

3.2 Introduction to Web Interface

The web interface of the SBC8000 consists of the main menu bar, navigation tree and detailed configuration interfaces. Click a button of the main menu bar and select a node of the navigation tree on the left, you will see a detailed display interface or configuration interface:

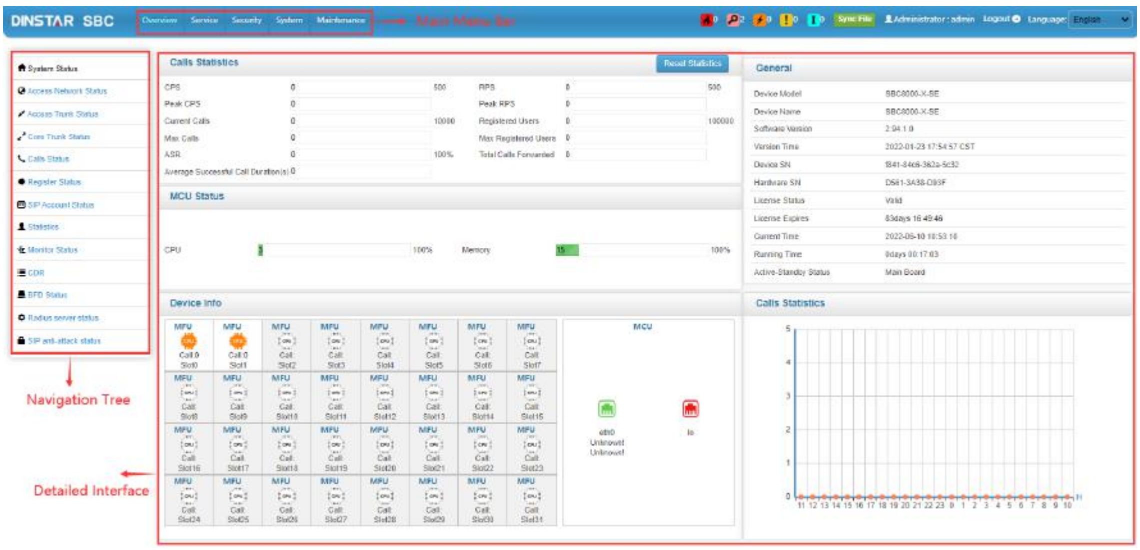


Figure 3-2-1 Structure of Web Interface

Table 3-2-1 Introduction to Web Interface

Index	**Item**	**Description**
1	Main Menu Bar	The main menu bar of SBC8000, including buttons of Overview, Service, Security, System and Maintenance
2	Navigation Tree	The navigation tree of each button of the main menu bar
3	Detailed Interface	The detailed configuration interface or display interface of a node under navigation tree
4	Language	Choose Chinese or English
5	Logout	Click logout, and you will exit the Web interface
6		To add configurations
7		To edit/modify configurations
8		To delete configurations

3.3 Configuration Flows

The following is the general configuration flows of SBC8000:

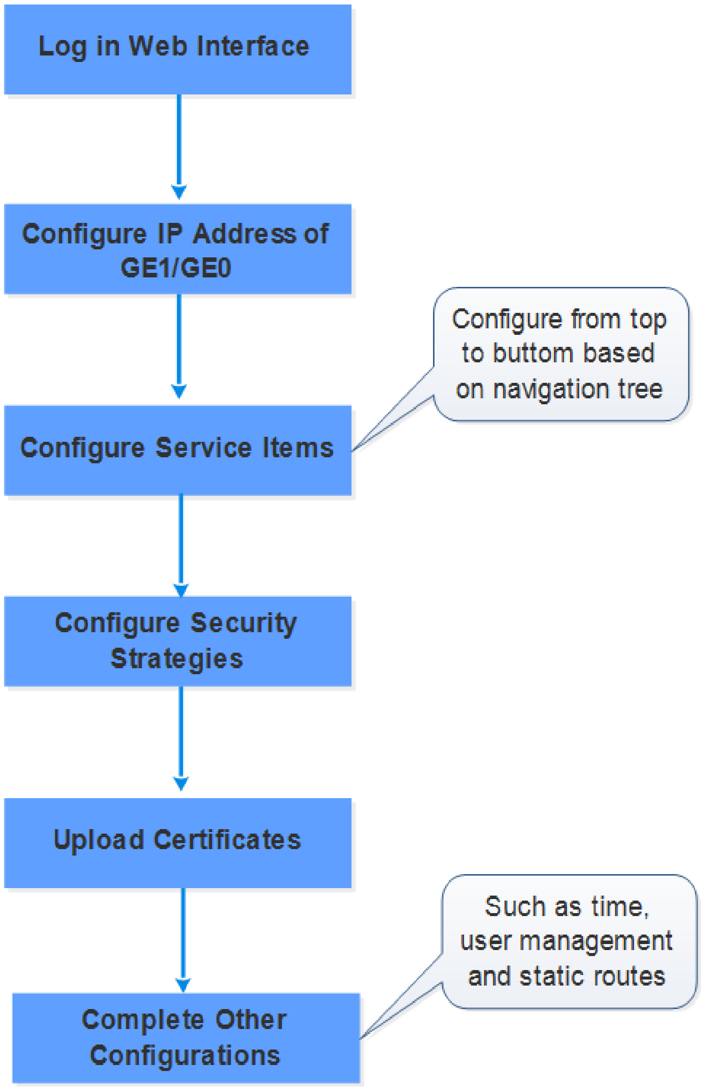


Figure 3-3-1 Configuration Flow

3.3.1 System Status

Log into the Web interface, and the **Overview -> System Status** page is displayed. On the page, call statistics and its graphic, device information, MCU(Main Control Unit) status as well as general information are shown.

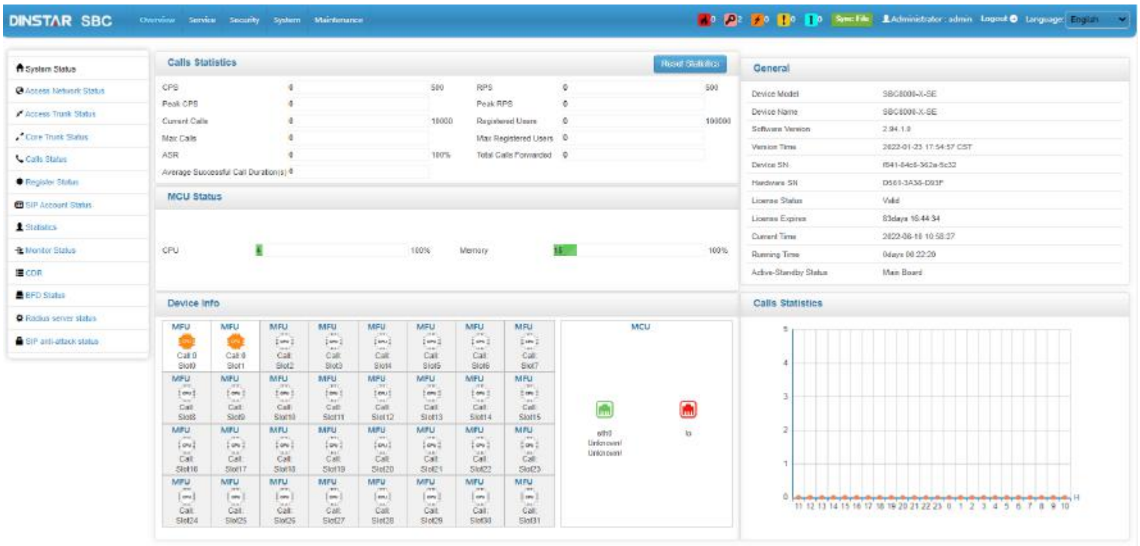


Figure 3-3-2 System Status

Table 3-3-1 Calls Statistics

CPS (Calls Per Second)	The number of new calls going through SBC8000 every second at current time
Peak CPS	The peak CPS (calls per second) since SBC8000 is booted up
Current Calls	The number of on-going calls at current time
Max Calls	The maximum number of concurrent calls since SBC8000 is booted up
ASR	ASR (Answer Success Rate) is a call success rate in telecommunication, which reflects the percentage of answered telephone calls with respect to the total call volume. ASR = answered call/total attempts of calls
Average Successful Call Duration(s)	Average Successful Call Duration is the duration of dividing the sum of the successful call durations by the number of successful calls since SBC8000 is

	booted up
RPS (Registrations Per Second)	The number of new requests for registrations every second at current time
Peak RPS	The peak RPS (registrations per second) since SBC8000 is booted up
Registered Users	The total number of registered users at current time
Max Registered Users	The maximum number of registrations that are simultaneously processed since SBC8000 is booted up
Total Calls Forwarded	The total number of legal call requests since SBC8000 is booted up

Table 3-3-2 MCU Status

CPU	The CPU occupancy rate at current time
Memory	The occupancy rate of memory at current time

Table 3-3-3 Device Information

MFU (Main Function Unit)	The status information of the MFU
MCU (Main Control Unit)	The status information for the Host Network

Table 3-3-4 General Information

Device Model	SBC8000-X-SE
Device Name	The name of the device, which can be modified on the ‘System System Management’ page

Software Version	The current software version No. running on SBC8000
Version Time	The compile time for this version
Device SN	The device serial number for this software version
Hardware SN	The hardware serial number of this software version
License Status	If the license is in its validity period, "Valid" will be displayed. If the license has expired, "Invalid" is shown
License Expires	The remaining time of license validity
Current Time	The current time of SBC8000, which can be modified or synchronized on the 'System Date & Time' page
Running time	The running time of the device since it is booted up
Active-Standby Status	Whether the system is in the mode of the single or the Active-Standby

3.3.2 Access Network Status

Terminal users are registered to SBC through access network. The status of access network is always “true”, which means the access network connection is available.

On the **Overview -> Access Network Status** page, detailed information about access network, including the status, name, CPS(Calls Per Second), number of registered users, ASR(Answered Success Ratio), number of calls that are being transcoded, number of current calls as well as number of total calls, are shown.

				Inbound Calls				Outbound Calls			
Name	Status	CPS	Registered	ASR	Transcoded	Current Calls	Total Calls	ASR	Transcoded	Current Calls	Total Calls
genpbx	true	0	0	0	0	0	0	0	0	0	0
test1	true	0	0	42	0	0	21	0	0	0	0
uc1000	true	0	0	0	0	0	0	0	0	0	0
uc8000	true	0	0	0	0	0	19	0	0	0	0

Figure 3-3-3 Access Network Status

Table 3-3-5 Access Network Status

Name	The name of the access network. It cannot be changed after the configuration is successfully applied
Status	The status of access network is always “true”, which means the access network is normal and available
CPS	The number of new calls going through the access network every second at current time
Registered	The total number of users that are successfully registered through the access network and are still in validity period
ASR	The ASR of the access network since the system is booted up; ASR = successful calls/total legal calling attempts

Transcoding	The number of calls that are being transcoded in the access network at current time
Current Calls	The number of current calls in the access network
Total Calls	The total number of legal calls since the system is booted up

Notes:

1. Calls are grouped into inbound calls and outbound calls. Inbound calls go from terminal users to SBC8000, while outbound calls are exactly the opposite.

2. Inbound calls and outbound calls have their own statistics of ASR, number of transcoded calls, number of current calls and number of total calls.

3.3.3 Access Trunk Status

Access SIP Trunk enables end users to connect with SBC8000 through SIP Trunk.

If both 'Registration' and 'Keepalive' are disabled for the SIP trunk on the **Service -> Access SIP Trunk** page, the status of the SIP trunk will be 'True'. If both 'Registration' and 'Keepalive' are enabled, the SIP trunk is successfully registered and meanwhile the option message for 'Keepalive' is successfully responded, the status of the SIP trunk will be 'True', otherwise, the status will be 'False'.

If only 'Registration' is enabled and meanwhile the SIP trunk is successfully registered, the status of the SIP trunk will be 'True', otherwise, the status will be 'False'. If only 'Keepalive' is enabled and meanwhile its option message is successfully responded, the status of the SIP trunk will be 'True', otherwise, the status will be 'False'.

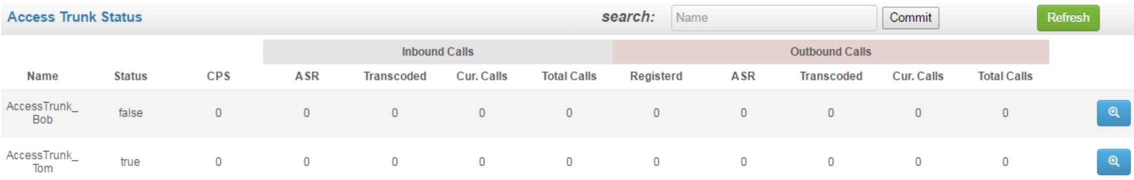


Figure 3-3-4 Access Trunk Status

Table 3-3-6 Access Trunk Status

Name	The name of the Access SIP Trunk. It cannot be changed after the configuration is successfully applied
Status	The status of the Access SIP Trunk. True: the Access SIP Trunk is connected normally and available; False: the Access SIP Trunk is disconnected and unavailable
CPS (Calls Per Second)	The number of new calls directed by the Access SIP Trunk every second at current time
ASR	The ASR of the Access SIP Trunk since the system is booted up; ASR = successful calls/total legal calling attempts
Transcoded	The number of calls that are being transcoded through the access SIP trunk at current time
Cur.Calls	The number of current calls routed by the access SIP trunk
Total Calls	The total number of legal calls routed by the access SIP trunk since the device is booted up

Registered	The total number of users that are successfully registered to SBC8000 by the help of the access SIP trunk and are still in validity period

Notes:

1. As for ASR, if the invite message of a call is successfully responded, we consider the call as a successful/answered call.

2. Calls are grouped into inbound calls and outbound calls. Inbound calls go from the terminals in access network to SBC8000, while outbound calls are exactly the opposite. Inbound calls and outbound calls have their own statistics of ASR, number of transcoded calls, number of current calls and number of total calls.

3.3.4 Core Trunk Status

Core network’s SIP trunk can connect SBC8000 to the core network through SIP Trunk.

If both ‘Registration’ and ‘Keepalive’ are disabled for the SIP trunk, the status of the SIP trunk will be ‘True’. If both ‘Registration’ and ‘Keepalive’ are enabled, the SIP trunk is successfully registered and meanwhile the option message for ‘Keepalive’ is successfully responded, the status of the SIP trunk will be ‘True’, otherwise, the status will be ‘False’.

If only ‘Registration’ is enabled and meanwhile the SIP trunk is successfully registered, the status of the SIP trunk will be ‘True’, otherwise, the status will be ‘False’. If only ‘Keepalive’ is enabled and meanwhile its option message is successfully responded, the status of the SIP trunk will be ‘True’, otherwise, the status will be ‘False’.

Name	Status	CPS	Inbound Calls ASR	Inbound Calls Transcoded	Inbound Calls Current Calls	Inbound Calls Total Calls	Outbound Calls Registerd	Outbound Calls ASR	Outbound Calls Transcoded	Outbound Calls Current Calls	Outbound Calls Total Calls
test	true	0	0	0	0	0	0	42	0	0	21
uc8000_server	true	0	0	0	0	0	0	0	0	0	19

Figure 3-3-5 Core Trunk Status

Table 3-3-7 Core Trunk Status

Name	The name of the core SIP trunk. It cannot be changed after the configuration is successfully applied
Status	The status of the core SIP trunk. True: the core SIP trunk is connected normally and available; False: the core SIP trunk is disconnected and unavailable
CPS (Calls Per Second)	The number of new calls routed by the core SIP trunk every second at current time
Registered	The total number of users that are successfully registered to SBC8000 by the help of the core SIP trunk and are still in validity period
ASR	The ASR of the core SIP trunk since the system is booted up; ASR = successful calls/total legal calling attempts
Transcoded	The number of calls that are being transcoded through the core SIP trunk at current time
Current Calls	The number of current calls routed by the core SIP trunk

Total Calls	The total number of legal calls routed by the core SIP trunk since the system is booted up

Notes:

1. As for ASR, if the invite message of a call is successfully responded, we consider the call as a successful/answered call.

2. Calls are grouped into inbound calls and outbound calls. Inbound calls go from core network to SBC8000, while outbound calls are exactly the opposite. Inbound calls and outbound calls have their own statistics of ASR, number of calls that are being transcoded, number of current calls and number of total calls.

3.3.5 Calls Status

On the **Overview Calls Status** page, the statuses, durations, caller number and callee number of current calls are displayed.

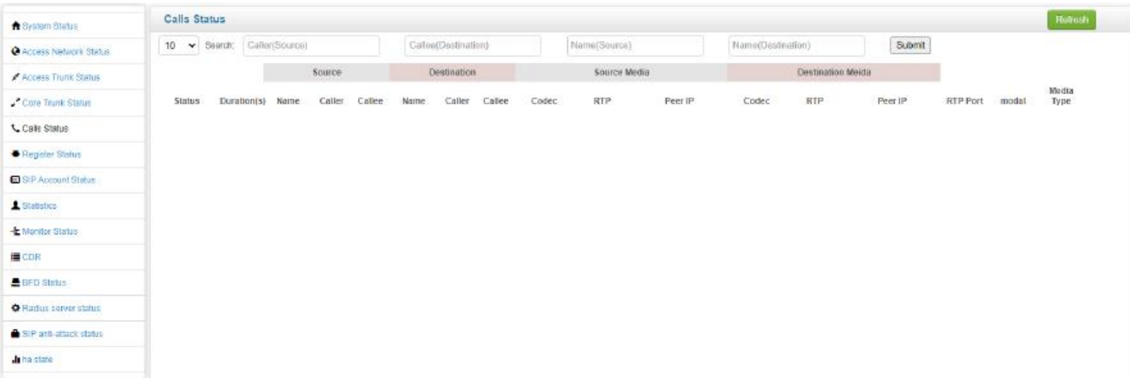


Figure 3-3-6 Calls Status

Table 3-3-8 Call Status

Status	**Init**: an invite request for calling is received and the call is initiated; **Outgoing**: the request for routing out the call is sent , and the system is waiting for response

	Early: the 18x response is received **Completed**: the 2xx response is received, and the system is waiting for the ack message **Answer**: the ack message is received, and the call is set up
Duration(s)	The duration of the call
Name	The name of the call, which will be used when the call goes through access network’s SIP trunk, core network’s SIP trunk or access network
Caller	The caller number of the call
Callee	The callee number of the call
Codec	The codec adopted by the call. If it is a transcoded call, the source codec is different from the destination codec
RTP	The number of RTP messages that received or sent. The statistics is collected every five seconds
Peer IP	The peer IP address and peer RTP port
RTP Port	The local RTP port of the call. If the RTP port is displayed as ‘0’, it means the RTP session has not been connected successfully
Model	Transfer or transcoding
Media Type	audio

3.3.6 Register Status

On the **Overview -> Register Status** page, the registration statuses of terminal users on SBC8000 are displayed.

Figure 3-3-7 Register Status

Table 3-3-9 Register Status

Status	Registering: SBC8000 has received the registration request send by terminal user, and is processing the request; Registered: The terminal user has been successfully registered and is in validity period
Username	The username of the terminal user, which will be used during registration
Name	Name (source): refers to the name of the access network where the registered terminal user is from; Name (destination): refers to the name of the core network' s SIP trunk where the registration goes to
Registered Interval	Registered Interval (source): the interval of registering to SBC8000 by terminal user Registered Interval (destination): the interval of registering to core network' s SIP trunk by SBC8000
IP Addr./NAT	IP Addr./NAT (source): the IP address and NAT address of terminal user IP Addr./NAT (destination): the IP address and NAT address of core network' s SIP trunk
Transport	The type of protocol used for registration

	(UDP/TCP/TLS/WSS)

3.3.7 SIP Account Status

On the **Overview -> SIP Account Status** page, the registration statuses of the SIP Account registered through the SBC8000 to the SIP server are displayed.

Figure 3-3-8 SIP Account Status

Table 3-3-10 SIP Account Status

Status	Registering: SBC8000 has send the registration request, and is processing the request; Registered: SBC8000 has received a successful registration response and is in validity period
Name	The name of the SIP account user group
Username	This username is used for softswitch registration
Endpoint	Endpoint is the trunk name associated with the SIP Account
Current Concurrency	Concurrent number of current user registrations
Max Concurrency	Maximum concurrent number of current user registrations
Times of Use	The number of times that the current user has been used, such as the number of calls

3.3.8 Statistics

3.3.9 Monitor Status

The **Overview -> Monitor Status** page displays parameters related to call quality and network quality, such as Network Jitter, Packet Loss Rate, Delay, and other parameters. SBC8000 supports setting conditions for search.

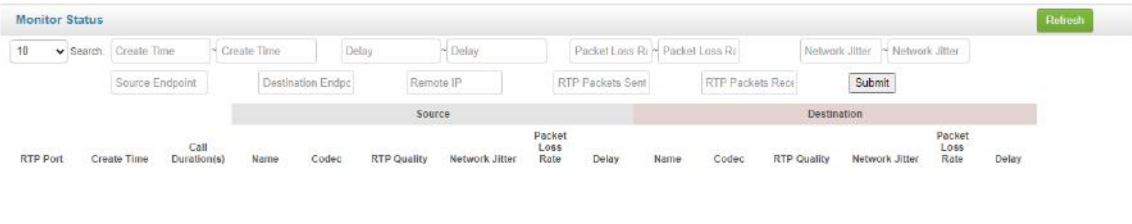


Figure 3-3-14 Monitor Status

Table 3-3-11 Monitor Status

RTP Port	Port of the media address during quality monitoring
Create Time	The time when the Monitor Status record was created, usually when the call ended
Call Duration(s)	The duration of the call
Name	The name of the trunk used when the call is made
Codec	The codec used after a successful call is made
RTP Quality	The number of received/sent RTP packets
Network Jitter	Packet Delay Variation (PDV), is a stuttering like effect in signal quality because of inconsistent packet delays in a data transmission
Packet Loss Rate	The Packet Loss Rate is the rate between the number of lost packets to the total number of packets sent.

Delay	The time that it takes for a message or packet to travel from one end of the network to the other

3.3.10 CDR

After enabling CDRs on the CDR Management page, users can check all the CDRs of the SBC on the CDR page. Users can set the conditions to search for details and export all the CDRs to local storage.

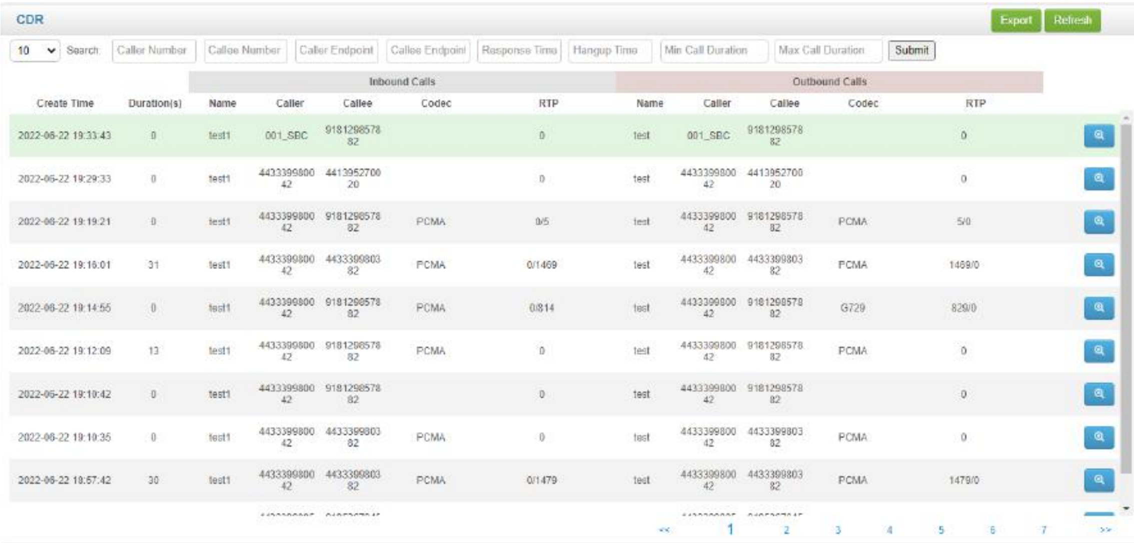


Figure 3-3-15 CDR

Table 3-3-12 CDR

Create Time	The time when the CDR was created, usually when the call ended
Duration(s)	The duration of the call
Name	The name of the trunk used when the call is made
Caller	The number of caller
Callee	The number of callee
Codec	The codec used after a successful call is made

RTP	The number of received/sent RTP packets

3.3.11 BFD Status

After dual-system hot standby is configured with BFD detection, this page displays the status of the BFD chain.

Figure 3-3-16 BFD Status

Table 3-3-13 BFD Status

Session Key	Session key detected by BFD
Current State	Current state of BFD
Running Time	The running time after the BFD configuration takes effect to the current time
Number of Chain Breaks	Total number of chain breaks after the successful configuration of BFD
Current Packet Loss Rate	The packet loss rate of the current BFD chain
Current Receiving Interval	Current interval of received data

3.3.12 Radius server status

The **Radius Server Status** page displays the information such as connection status and CDRs between the device and radius server.

Figure 3-3-17 Radius Server Status

Table 3-3-14 Radius Server Status

server IP	IP address of the Radius server
Remote accounting port	Accounting port of the Radius server
Status	Status of the Radius server
Successfully sent the number of CDRs	Number of successfully sent CDRs to radius server

3.3.13 SIP anti-attack status

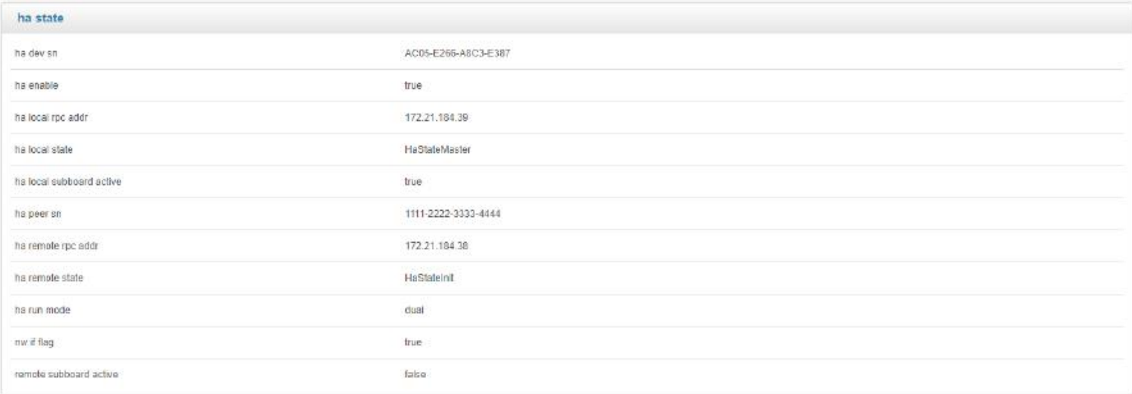
The **SIP anti-attack status** page displays the blocked objects that are restricted to the SIP Anti-Attack Policy and the block expiration date.

Figure 3-3-18 SIP anti-attack status

Table 3-3-15 SIP anti-attack status

Block object	IP addresses, SIP accounts, trunks, etc. that are restricted by SIP anti-attack policies
Block expire date	Unblock time of block objects

3.3.14 ha state



ha state

ha dev sn	AC05-E266-A8C3-E387
ha enable	true
ha local rpc addr	172.21.184.39
ha local state	HaStateMaster
ha local subboard active	true
ha peer sn	1111-2222-3333-4444
ha remote rpc addr	172.21.184.38
ha remote state	HaStateInit
ha run mode	dual
nw if flag	true
remote subboard active	false

Figure 3-3-19 ha state

Table 3-3-15 ha state

ha dev sn	Serial number of the local device under the Active-Standby mode
ha enable	Display HA state when dual Active-Standby mode is enabled
ha local rpc addr	The IP address of the management port of the local device
ha local state	Whether the local device is the master or the slave state (HaStateSlave: slave; HaStateMaster: master)
ha local subboard active	The activated flag of local subboard. The dsp is activated and displayed as true, otherwise it is displayed as false.
ha peer sn	Serial number of the peer device under the Active-Standby mode
ha remote rpc addr	he IP address of the management port of the

	remote device
ha remote state	Whether the remote device is the master or the slave state (HaStateSlave: slave; HaStateMaster: master)
ha run mode	Whether the system is in HA mode or not. The dual indicates that it is in HA mode, and disable indicates that it is not.
nw if flag	Status of the network interface for active and standby connection
remote subboard active	The activated flag of remote subboard. The dsp is activated and displayed as true, otherwise it is displayed as false.

3.4 Service

3.4.1 Access Network

On the **Service -> Access Network** page, user can configure the parameters of access network, which will be used when terminal users are registered to softswitch through the SBC.

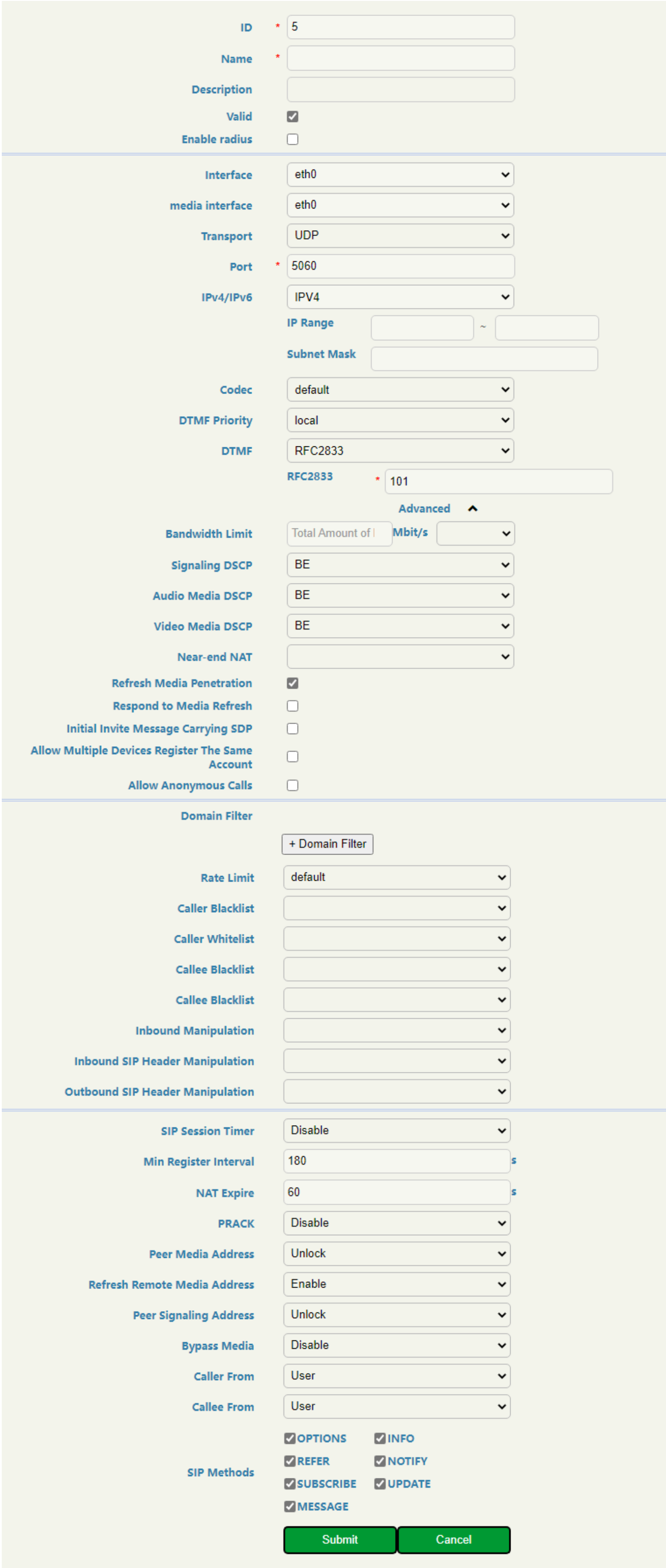


Figure 3-4-1 Configure Parameters of Access Network

Table 3-4-1 Access Network

Name	The name of the access network. It cannot be modified after the access network has been added successfully
Description	The description of the access network
Valid	This option is enabled by default, the access network is disabled when it is unchecked.
Enable radius	This option is off by default, select it to enable the radius server to send CDRs
Interface	The interface of the access network
Media Interface	The media interface of the access network
Transport	Select a transport protocol for the access network. It can be UDP, TCP, TLS or WSS
Port	The access network’s SIP listening port on the Ethernet interface of the SBC, and the port number is unique on this interface
IPv4/IPv6	Select a network protocol for the access network. It can be IPv4 or IPv6. By default, the network protocol is IPv4
IP Range	Configure the range of legal IP addresses that send out SIP request can be received by the
Subnet Mask	The subnet mask of the IP range
Codec	Configure the supported codec from inbound or

	outbound calls of access network. Please go to **Service -> Codec Profile** to get more details
DTMF Priority	The DTMF Priority of Access Network. It can be local or remote
DTMF	DTMF is short for Dual Tone Multi Frequency; There are three DTMF modes, including SIP Info, INBAND, RFC2833; If the DTMF mode of an access network differs from that of core network, SBC8000 will convert it through DSP
Bandwidth Limit	Maximum bandwidth of this access network
Signaling DSCP	The DSCP is to ensure QoS of the communication. It is encoded in the 8 identification bytes in the IP header of the packet to classify the services and distinguish the priorities. The default Signaling DSCP is BE, and there are 14 Signaling DSCPs.
Audio Media DSCP	The default Audio Media DSCP is BE, and there are 14 Signaling DSCPs.
Video Media DSCP	The default Video Media DSCP is BE, and there are 14 Signaling DSCPs.
Near-end NAT	Near-end NAT defaults to disabled. If it is enabled, the contact IP address contained in SIP messages sent out by SBC8000 will be turned into the

	outbound IP address of public network. If NAT is enabled, you need to fill in the outbound IP address of public network.
Refresh Media Penetration	Pass-through sessions with SDP to refresh reinvite and update messages
Respond to Media Refresh	When more than one codec is received, the final codec of the SBC8000 is sent to the remote side with a reinvite message
Initial Invite Message Carrying SDP	The initial invite message sent by the SBC carrying SDP
Allow Multiple Devices Register The Same Account	Single account supports multiple terminal registration
Allow Anonymous Calls	Allow end users to call anonymously
Domain Filter	Receive registration requests only for the configured domain name
Rate Limit	Configure the RPS, CPS and Max Media Sessions for this access network Please go to **Service -> Rate Limit** to get more details
Caller/Callee Blacklist	Select a Caller/Callee blacklist for the access network. Calls given by the caller numbers on the blacklist will be refused to go through the access network. Please go to **Service ->Blacklist & Whitelist**

	->Blacklist to get more details
Caller/Callee Whitelist	Select a Caller/Callee whitelist for the access network. Calls initiated by the caller numbers on the whitelist will be allowed to go through the access network. Please go to **Service ->Blacklist & Whitelist ->Whitelist** to get more details If no black list and white list are selected for the access network, all calls are allowed to go through the access network
Inbound Manipulation	Select a number manipulation rule or a number pool for the access network. When a call coming into the access network matches the manipulation rule, its number will be manipulated. Please go to **Service -> Number Manipulation/ Number Pool** to get more details
Inbound SIP Header Manipulation	Select a SIP header manipulation rule for inbound calls of the access network. If a call matches the manipulation rule, the SIP header of the messages related to the call will be manipulated when it comes into the access network. Please go to **Service -> SIP Header Manipulation** to get more details
Outbound SIP Header Manipulation	Select a SIP header manipulation rule for outbound calls of the access network. If a call matches the manipulation rule, the SIP header of the messages related to the call will be manipulated when it goes

	out the access network. Please go to **Service -> SIP Header Manipulation** to get more details
SIP Session Timer	Session timer is a mechanism to keep activating sessions. If 'Supported' is selected, SBC8000 will send 'reinvite' messages to keep activating sessions within the configured duration. If no messages are detected within the configured duration, sessions will be considered as 'ended', and then will be disconnected. If 'Require' is selected, the callee side of a call passing through the access network also needs to support session timer.
Min Register Interval	Minimum session duration is used to negotiate with the session timer on the callee side
NAT Expire	If a terminal is in private network and sends out messages through NAT, the registration time responded by SBC8000 will automatically turned into the time configured here. The value of 'NAT Expire'
PRACK	PRACK (Provisional Response ACKnowledgement): provide reliable provisional response messages. Disable: INVITE request and 1xx response sent out by SBC8000 will not include 100rel tag by default; Support: INVITE request and 1xx response sent out

	by SBC8000 will include 100rel tag in Supported header; Require: INVITE request and 1xx response sent out by SBC8000 will include 100rel tag in Require header; if the peer does not support 100rel, it will automatically reject INVITE request with 420; if the peer supports 100rel. it will send PRACK request to acknowledge the response.
Peer Media Address	Lock: when the peer device works at public network, media address carried in SDP (Session Description Protocol) message is locked; when the peer device works at private network, the address that sends 30 messages continuously are locked. Unlock: remote address sending media messages is not locked.
Refresh Remote Media Address	If this parameter is enabled, the remote address receiving media messages will be refreshed.
Peer Signaling Address	Lock: when a calling account is successfully registered, the access network only receives those calls from the registered address of the caller.
Bypass Media	After bypass media is enabled, the RTP of the terminal under the same NAT will not be forwarded by SBC8000
Caller From	User: the USER field of FROM header of INVITE message is extracted as caller number Display: the DISPLAY field of FROM header of

	INVITE message is extracted as caller number
Callee From	User: the USER field of TO header of INVITE message is extracted as callee number; Display: the DISPLAY field of TO header of INVITE message is extracted as callee number; Request-uri: the USER NUMBER in REQUEST-URI of INVITE message is extracted as callee number;
SIP Methods	Configure the SIP request methods that can be accepted by the access network. If a SIP request method is not enabled, the system will reject the corresponding SIP request. By default, the INVITE request, REGISTER request and SESSION DISCONNECT request are accepted.

Notes:

When you configure static NAT, the default SIP and RTP ports can be empty. If you have mapped the ports to the firewall, you need to configure them according to the mapping rules. For example:

1. SIP Port: A trunk has a local 5061 port, but the firewall maps port 5061 to port 8888. Then the SIP port of the static NAT should be configured to 8888.

2. The default RTP start port for the SBC is 32768. If the firewall maps ports 32768-50000 to 12768-30000, then the static NAT's RTP start port should be configured to 12768. This means that the RTP start port of static NAT is actually based on port 32768, and then the port will be changed according to the firewall mapping rules.

3.4.2 Access SIP Trunk

On the **Service Access SIP Trunk** page, you can configure the server and related parameters of the access network terminal that the SBC is connected to through the trunk.

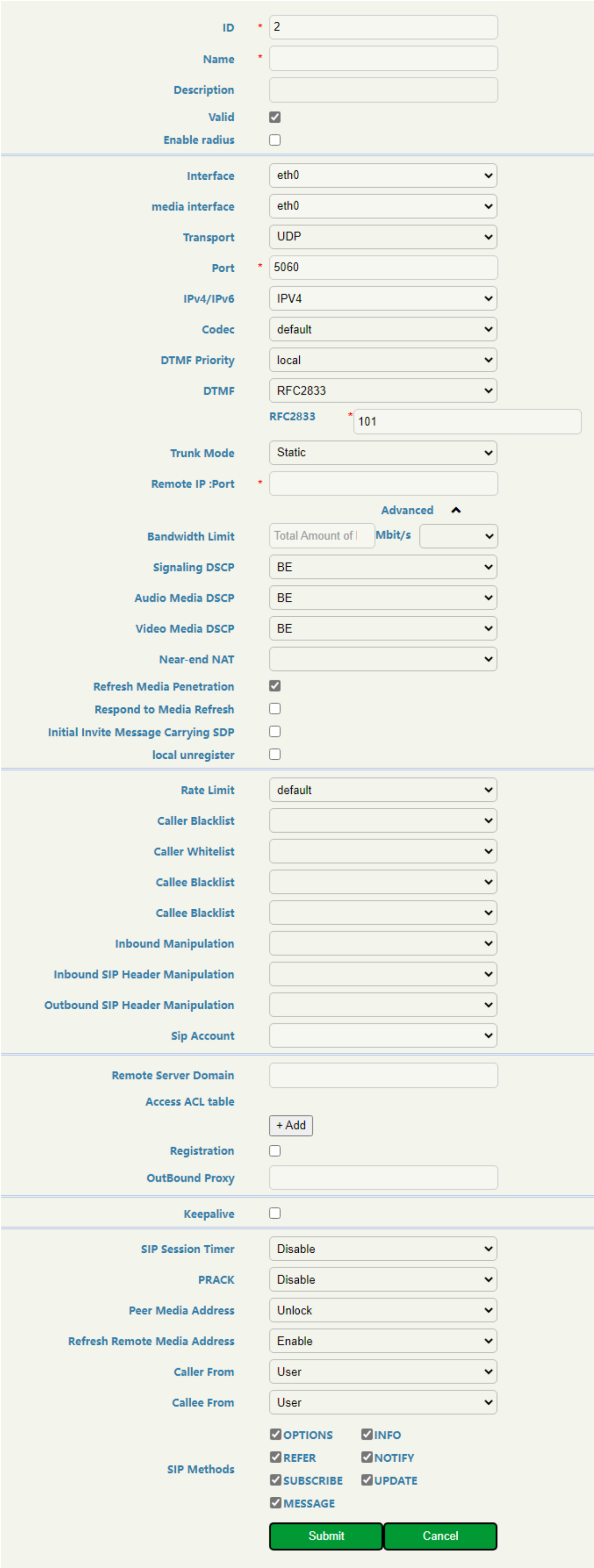


Figure 3-4-2 Configure Access SIP Trunk

Table 3-4-2 Access SIP Trunk

Name	The name of the access SIP trunk. It cannot be modified after the access SIP trunk has been added successfully
Description	The description of the access SIP trunk
Valid	This option is enabled by default, the Access SIP Trunk is disabled when it is unchecked.
Enable radius	This option is off by default, select it to enable the radius server to send CDRs
Interface	The network interface or VLAN interface of the Access SIP Trunk to receive/send Data
media interface	The network interface or VLAN interface of the Access SIP Trunk to receive/send Media Data
Transport	Select a transport protocol for the access SIP trunk. It can be UDP, TCP or TLS
Port	The access SIP trunk’s SIP listening port on the Ethernet interface of SBC
IPv4/IPv6	Select a network protocol for the access SIP trunk. It can be IPv4 or IPv6. By default, the network protocol is IPv4
Codec	The codecs that the access SIP trunk supports. Please go to **Service -> Codec Profile** to get more details

DTMF Priority	The DTMF Priority of Access SIP Trunk. It can be local or remote
DTMF	DTMF is short for Dual Tone Multi Frequency; There are three DTMF modes, including SIP Info, Inband, RFC2833; If the DTMF mode of an access SIP trunk differs from that of core network, SBC8000 will convert it through DSP
Trunk Mode	**When SBC is connected to IMS,** **Static**: you need to manually configure the IP address and port of the peer device, for example, 192.168.2.159:5060 Remote domain name: the domain name of the peer **Dynamic**: the access SIP trunk works as a server, and you need to configure username, authentication ID and password for the SIP trunk, which will be used when a peer device tries to register to the SIP trunk. If the peer device registers to the SIP trunk successfully, the status of the SIP trunk will be ‘True’. If the peer device fails to register or does not register to the SIP trunk, the status of the SIP trunk will be ‘Flase’.
Bandwidth Limit	Maximum bandwidth of this Access SIP Trunk
Signaling DSCP	The DSCP is to ensure QoS of the communication. It is encoded in the 8 identification bytes in the IP

	header of the packet to classify the services and distinguish the priorities. The default Signaling DSCP is BE, and there are 14 Signaling DSCPs.
Audio Media DSCP	The default Audio Media DSCP is BE, and there are 14 Signaling DSCPs.
Video Media DSCP	The default Video Media DSCP is BE, and there are 14 Signaling DSCPs.
Near-end NAT	Near-end NAT is disabled by default. If it is enabled, the contact IP address contained in SIP messages sent out by SBC will be turned into the outbound IP address of public network. If NAT is enabled, you need to fill in the outbound IP address of public network.
Refresh Media Penetration	Pass-through sessions with SDP to refresh reinvite and update messages
Respond to Media Refresh	When more than one codec in SDP is received, the final codec of the SBC will be sent to the remote side with a reinvite message
Initial Invite Message Carrying SDP	The initial invite message sent by the SBC carrying SDP
local unregister	The SBC processes the terminal's unregister message and does not forward it to the SIP Server.

Rate Limit	The maximum RPS(registrations per second), CPS(calls per second) and total call volume of the access SIP trunk. Please go to **Service -> Rate Limit** to get more details
Caller/Callee Blacklist	Select a blacklist for the access SIP trunk. Calls given by the caller numbers on the blacklist cannot be routed by the access SIP trunk. Please go to **Service -> Black & White List** to get more details
Caller/Callee Whitelist	Select a whitelist for the access SIP trunk. Calls initiated by the caller numbers on the whitelist will be directed by the access SIP trunk. Please go to **Service -> Black & White List** to get more details If no black list and white list are selected for the access SIP trunk, all calls can be routed by the access SIP trunk.
Inbound Manipulation	Select a number manipulation rule or a number pool for the access SIP trunk. When a call routed by the SIP trunk matches the manipulation rule, its number will be manipulated. Please go to **Service -> Number Manipulation/ Number Pool** to get more details
Inbound SIP Header Manipulation	Select a SIP header manipulation rule for inbound calls of the access SIP trunk. If a call matches the

	manipulation rule, the SIP header of the messages related to the call will be manipulated when it comes into the access SIP trunk. Please go to **Service -> SIP Header Manipulation** to get more details
Outbound SIP Header Manipulation	Select a SIP header manipulation rule for outbound calls of the access SIP trunk. If a call matches the manipulation rule, the SIP header of the messages related to the call will be manipulated when it goes out the access SIP trunk. Please go to **Service -> SIP Header Manipulation** to get more details
SIP Account	Configure SIP Account registration information from the SBC to the server Please go to **Service -> SIP Account** to get more details
Remote Server Domain	Configure the domain name of the remote server
Access ACL table	Table of IP addresses and ports allowed to be accessed, and support for regular expressions
Registration	When ‘Server IP Type’ is configured as ‘Static’, registration will be displayed. If registration is enabled, the access IP trunk will be registered to the configured peer address and port, and the status of the access SIP trunk will become ‘Ture’. Otherwise, the status is ‘False’. For the status of Access SIP trunk, please go to

	Overview-> Access Trunk Status to get more details
OutBound Proxy	Configure the IP address of the proxy server of the access trunk
Keepalive	If 'Keepalive' is disabled, the system will not detect whether the access SIP trunk's peer device (generally it is the access network server) is reachable or not. If it is enabled, option message will be sent to detect the access network server is reachable. If response is received, it means the peer device is reachable, and the status of the access SIP trunk is 'True'. Otherwise, the status will be 'False'. For the status of Access SIP trunk, please go to **Overview-> Access Trunk Status** to get more details
SIP Session Timer	Session timer is a mechanism to keep activating sessions. If 'Supported' is selected, SBC will send 'reinvite' messages to keep activating sessions within the configured duration. If no messages are detected within the configured duration, sessions will be considered as 'ended', and then will be disconnected. If 'Require' is selected, the callee side of a call passing through the access SIP trunk also needs to support session timer.

PRACK	PRACK (Provisional Response ACKnowledgement): provide reliable provisional response messages. Disable: INVITE request and 1xx response sent out by SBC will not include 100rel tag by default; Support: INVITE request and 1xx response sent out by SBC will include 100rel tag in Supported header; Require: INVITE request and 1xx response sent out by SBC will include 100rel tag in Require header; if the peer does not support 100rel, it will automatically reject INVITE request with 420; if the peer supports 100rel. it will send PRACK request to acknowledge the response.
Peer Media Address	Lock: when the peer device works at public network, media address carried in SDP (Session Description Protocol) message is locked; when the peer device works at private network, the address that sends 30 messages continuously are locked. Unlock: remote address sending media messages is not locked.
Refresh Remote Media Address	If this parameter is enabled, the remote address receiving media messages will be refreshed.
Caller From	User: the USER field of FROM header of INVITE message is extracted as caller number Display: the DISPLAY field of FROM header of INVITE message is extracted as caller number
Callee From	User: the USER field of TO header of INVITE

	message is extracted as callee number; Display: the DISPLAY field of TO header of INVITE message is extracted as callee number; Request-uri: the USER NUMBER in REQUEST-URI of INVITE message is extracted as callee number;
SIP Methods	Configure the SIP request methods that can be accepted by the access SIP trunk. If a SIP request method is not enabled, the system will reject the corresponding SIP request. By default, the INVITE request, REGISTER request and SESSION DISCONNECT request are always accepted.

3.4.3 Core SIP Trunk

On the **Service -> Core SIP Trunk** page, you can configure the SIP/IPPBX server and related parameters, and then the SBC system can be connected to the Core Network (Internal Network) through this trunk.

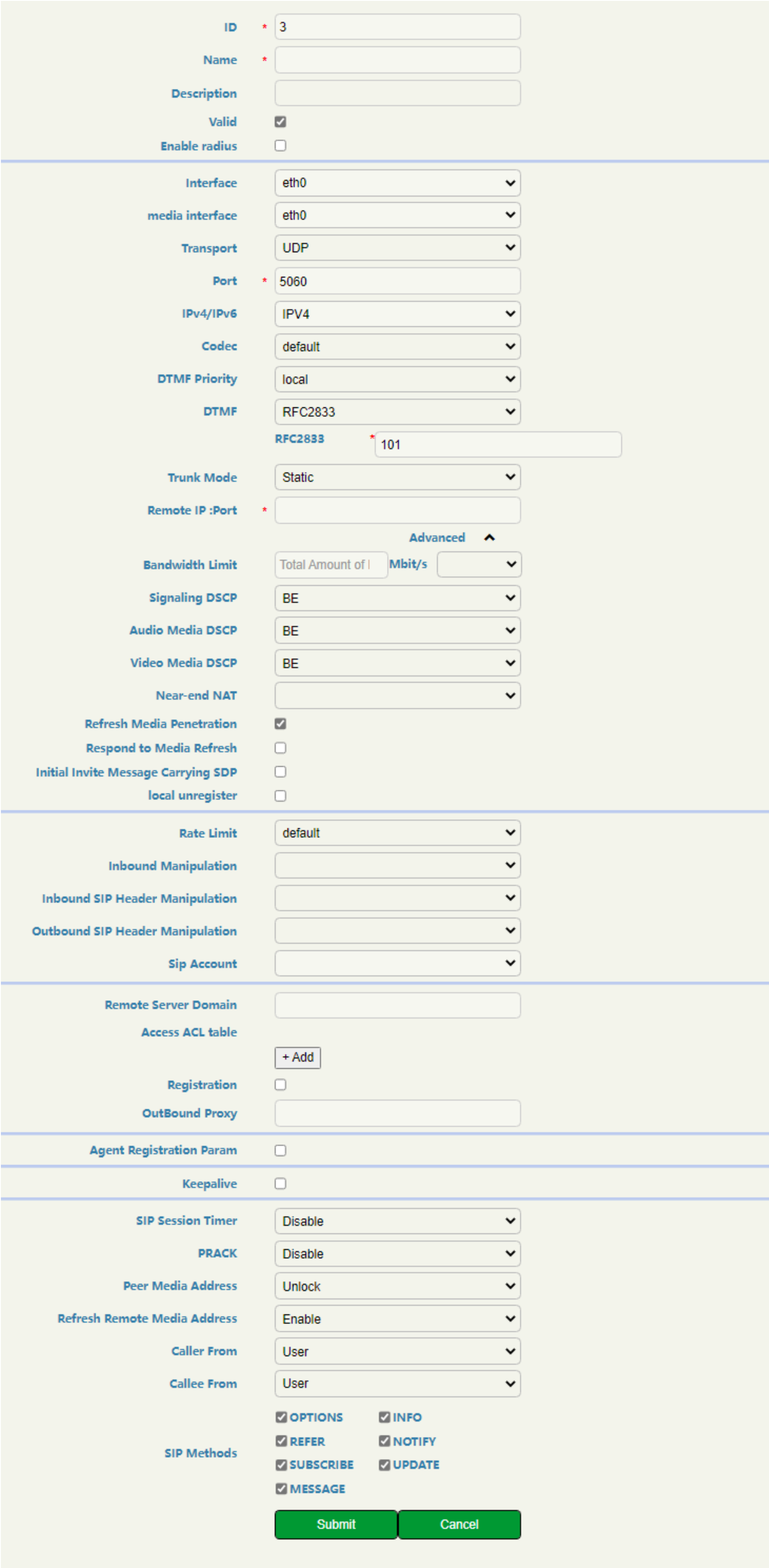


Figure 3-4-3 Core SIP Trunk

Table 3-4-3 Core SIP Trunk

Name	The name of the Core SIP Trunk. It cannot be modified after the Core SIP Trunk has been added successfully
Description	The description of the Core SIP Trunk
Valid	This option is enabled by default, the Core SIP Trunk is disabled when it is unchecked.
Enable radius	This option is off by default, select it to enable the radius server to send CDRs
Interface	The network interface or VLAN interface of the Core SIP Trunk to receive/send Data
media interface	The network interface or VLAN interface of the Core SIP Trunk to receive/send Media Data
Transport	Select a transport protocol for the Core SIP Trunk. It can be UDP, TCP or TLS
Port	The Core SIP Trunk’s SIP listening port on the Ethernet interface of SBC
IPv4/IPv6	Select a network protocol for the Core SIP Trunk. It can be IPv4 or IPv6. By default, the network protocol is IPv4
Codec	The codecs that the Core SIP Trunk supports. Please go to **Service -> Codec Profile** to get more details
DTMF Priority	The DTMF Priority of Core SIP Trunk. It can be local or

	remote
DTMF	DTMF is short for Dual Tone Multi Frequency; There are three DTMF modes, including SIP Info, Inband, RFC2833; If the DTMF mode of an Core SIP Trunk differs from that of core network, SBC will convert it through DSP
Trunk Mode	**When SBC is connected to IMS,** **Static**: you need to manually configure the IP address and port of the peer device, for example, 192.168.2.159:5060 Remote domain name: the domain name of the peer **Dynamic**: the Core SIP Trunk works as a server, and you need to configure username, authentication ID and password for the SIP trunk, which will be used when a peer device tries to register to the SIP trunk. If the peer device registers to the SIP trunk successfully, the status of the SIP trunk will be ‘True’. If the peer device fails to register or does not register to the SIP trunk, the status of the SIP trunk will be ‘Flase’.
Bandwidth Limit	Maximum bandwidth of this Core SIP Trunk
Signaling DSCP	The DSCP is to ensure QoS of the communication. It is encoded in the 8 identification bytes in the IP header of the packet to classify the services and distinguish the priorities. The default Signaling DSCP is BE, and there are 14 Signaling DSCPs.

Audio Media DSCP	The default Audio Media DSCP is BE, and there are 14 Signaling DSCPs.
Video Media DSCP	The default Video Media DSCP is BE, and there are 14 Signaling DSCPs.
Near-end NAT	Near-end NAT is disabled by default. If it is enabled, the contact IP address contained in SIP messages sent out by SBC will be turned into the outbound IP address of public network. If NAT is enabled, you need to fill in the outbound IP address of public network.
Refresh Media Penetration	Pass-through sessions with SDP to refresh reinvite and update messages
Respond to Media Refresh	When more than one codec in SDP is received, the final codec of the SBC will be sent to the remote side with a reinvite message
Initial Invite Message Carrying SDP	The initial invite message sent by the SBC carrying SDP
local unregister	The SBC processes the terminal's unregister message and does not forward it to the SIP Server.
Rate Limit	The maximum RPS(registrations per second), CPS(calls per second) and total call volume of the access SIP trunk. Please go to **Service -> Rate Limit** to get more details

Inbound Manipulation	Select a number manipulation rule or a number pool for the Core SIP Trunk. When a call routed by the SIP trunk matches the manipulation rule, its number will be manipulated. Please go to **Service -> Number Manipulation/ Number Pool** to get more details
Inbound SIP Header Manipulation	Select a SIP header manipulation rule for inbound calls of the Core SIP Trunk. If a call matches the manipulation rule, the SIP header of the messages related to the call will be manipulated when it comes into the Core SIP Trunk. Please go to **Service -> SIP Header Manipulation** to get more details
Outbound SIP Header Manipulation	Select a SIP header manipulation rule for outbound calls of the Core SIP Trunk. If a call matches the manipulation rule, the SIP header of the messages related to the call will be manipulated when it goes out the Core SIP Trunk. Please go to **Service -> SIP Header Manipulation** to get more details
SIP Account	Configure SIP Account registration information from the SBC to the server Please go to **Service -> SIP Account** to get more details
Remote Server Domain	Configure the domain name of the remote server

Access ACL table	Table of IP addresses and ports allowed to be accessed, and support for regular expressions
Registration	When ‘Server IP Type’ is configured as ‘Static’, registration will be displayed. If registration is enabled, the Core SIP Trunk will be registered to the configured peer address and port, and the status of the Core SIP Trunk will become ‘Ture’. Otherwise, the status is ‘False’. For the status of Core SIP Trunk, please go to **Overview->Core SIP Trunk Status** to get more details
OutBound Proxy	Configure the IP address of the proxy server of the Core SIP Trunk
Agent Registration Param	Configure agent registration parameters, including Registered Interval and Timeout coefficient
Keepalive	If ‘Keepalive’ is disabled, the system will not detect whether the Core SIP Trunk’s peer device (generally it is the core network server) is reachable or not. If it is enabled, option message will be sent to detect the core network server is reachable. If response is received, it means the peer device is reachable, and the status of the Core SIP Trunk is ‘True’. Otherwise, the status will be ‘False’. For the status of Core SIP Trunk, please go to **Overview-> Access Trunk Status** to get more details
SIP Session Timer	Session timer is a mechanism to keep activating sessions.

	If 'Supported' is selected, SBC will send 'reinvite' messages to keep activating sessions within the configured duration. If no messages are detected within the configured duration, sessions will be considered as 'ended', and then will be disconnected. If 'Require' is selected, the callee side of a call passing through the Core SIP Trunk also needs to support session timer.
PRACK	PRACK (Provisional Response ACKnowledgement): provide reliable provisional response messages. Disable: INVITE request and 1xx response sent out by SBC will not include 100rel tag by default; Support: INVITE request and 1xx response sent out by SBC will include 100rel tag in Supported header; Require: INVITE request and 1xx response sent out by SBC will include 100rel tag in Require header; if the peer does not support 100rel, it will automatically reject INVITE request with 420; if the peer supports 100rel. it will send PRACK request to acknowledge the response.
Peer Media Address	Lock: when the peer device works at public network, media address carried in SDP (Session Description Protocol) message is locked; when the peer device works at private network, the address that sends 30 messages continuously are locked. Unlock: remote address sending media messages is

	not locked.
Refresh Remote Media Address	If this parameter is enabled, the remote address receiving media messages will be refreshed.
Caller From	User: the USER field of FROM header of INVITE message is extracted as caller number Display: the DISPLAY field of FROM header of INVITE message is extracted as caller number
Callee From	User: the USER field of TO header of INVITE message is extracted as callee number; Display: the DISPLAY field of TO header of INVITE message is extracted as callee number; Request-uri: the USER NUMBER in REQUEST-URI of INVITE message is extracted as callee number;
SIP Methods	Configure the SIP request methods that can be accepted by the Core SIP Trunk. If a SIP request method is not enabled, the system will reject the corresponding SIP request. By default, the INVITE request, REGISTER request and SESSION DISCONNECT request are always accepted.

3.4.4 Routing Profile

3.4.4.1 SIP Trunk Group

On the **Routing Profiles -> SIP Trunk Group** page, you can group several access SIP trunks or core SIP trunks, and then set a strategy (backup or load balance) for choosing which trunk will be used under a trunk group when a call comes in.

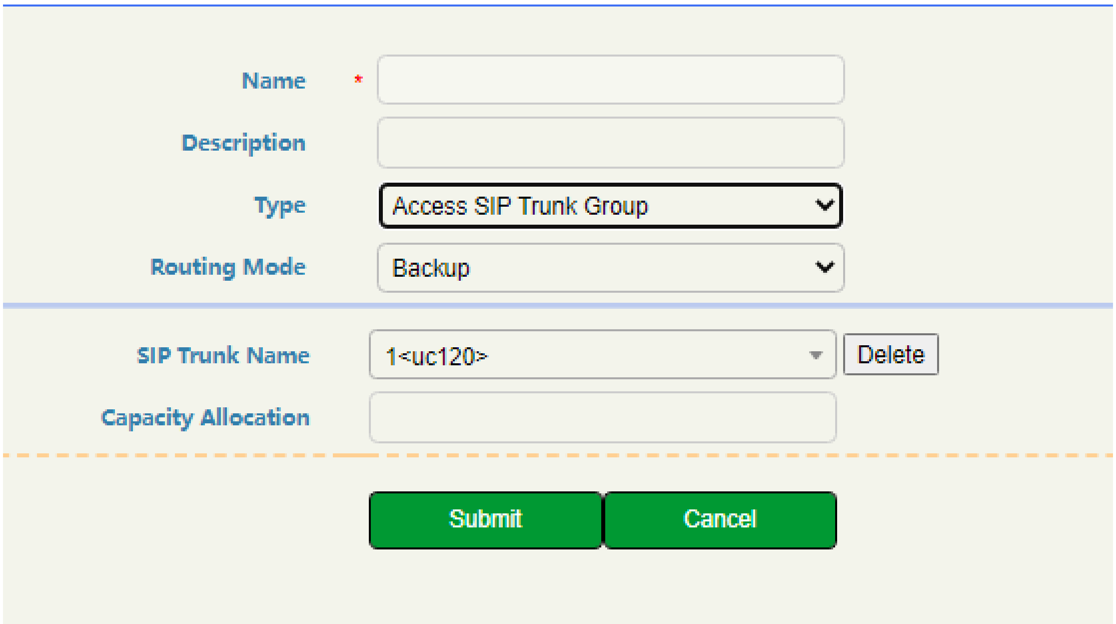


Figure 3-4-4 Configure SIP Trunk Group

Table 3-4-4 SIP Trunk Group

Name	The name of the SIP trunk group. It cannot be modified after the SIP trunk group has been added successfully
Description	The description of the SIP trunk group
Trunk Type	It can be access SIP trunk or core SIP trunk.
Routing Mode	The strategy for choosing which truck will be used under a trunk group when a call comes in. **Backup**: if the status of the first SIP trunk is ‘True’, the call will be always routed by the first SIP trunk. If the status of the first SIP trunk is ‘False’, the call will be routed by the next available SIP trunk. **Load Balance**: Trunk will be chosen according to the weight configured for it. For example, assuming the weight of a SIP trunk is 60% and that of the other SIP trunk in the same group is 40%, if there are 10 calls comes in, 6 calls will be routed by the first SIP trunk,

	and 4 calls will be routed by the second SIP trunk.
Trunk Name	The name of the access SIP trunk or core SIP trunk included in the trunk group
Capacity Allocation	Configure the capacity allocation of the relevant trunk

3.4.4.2 Call Routing

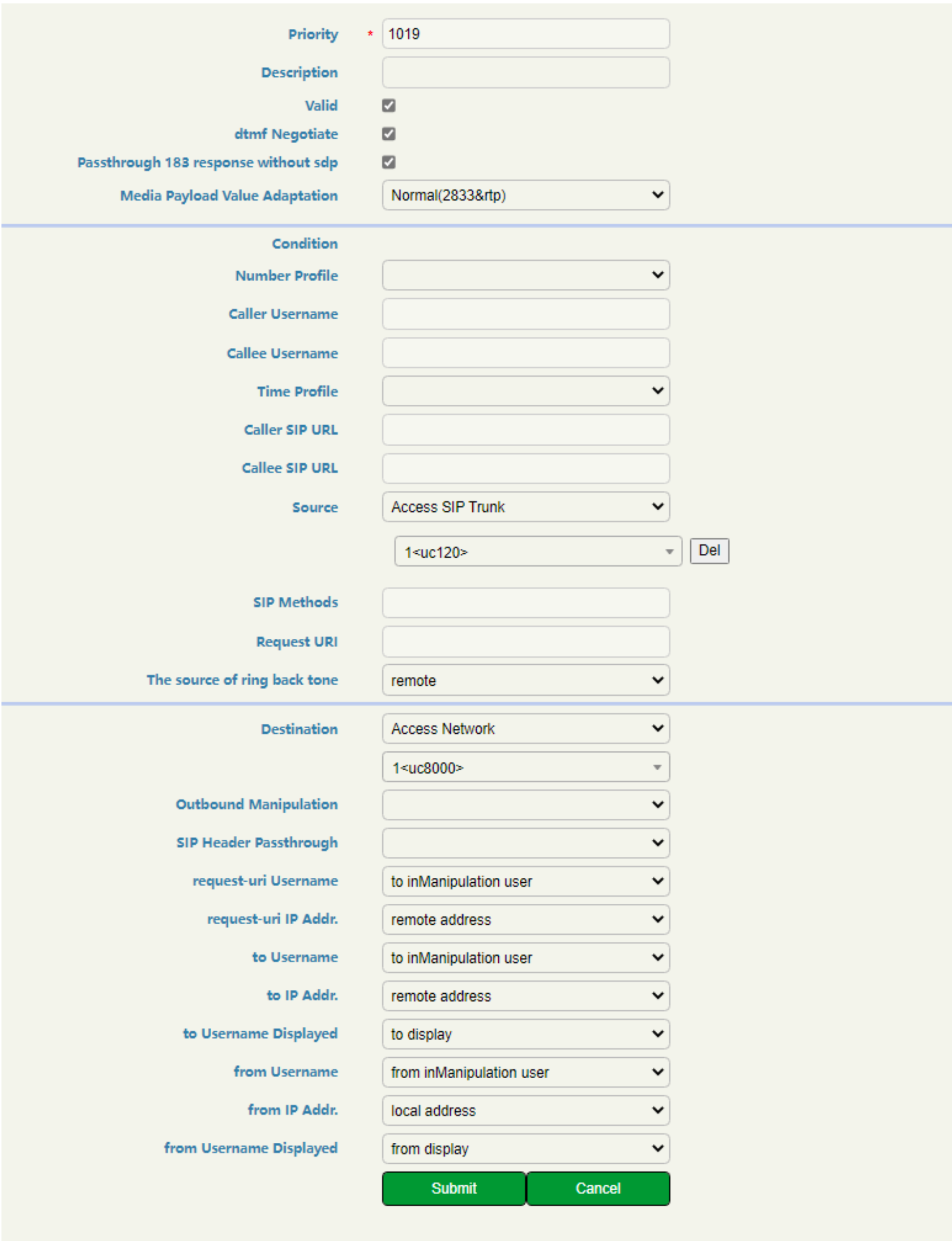


Figure 3-4-5 Call Routing

Table 3-4-5 Call Routing

Priority	The priority of the route, which determines the priority for a call to choose the route; the higher value, the lower priority.
Description	The description of the route, which is generally used to identify the route
Valid	The option is enabled by default, and when unchecked, the route is disabled.
dtmf Negotiate	Negotiation of DTMF after the this enabled, otherwise no DTMF negotiation
Passthrough 183 response without sdp	Enable or disable Passthrough 183 response without SDP
Media Payload Value Adaptation	Configure whether the payload value is adapted to 2833&RTP, only 2833 or none.
Number Profile	The number profile set for matching the route. If the caller number or the called number of a call matches with a number in this profile, the call will be routed by the route. This parameter is optional to fill in. Please go to **Service -> Number Profile** to get more details
Caller Username	The caller number set for matching the route, which supports regular expression. If the caller number of a call matches with this number, the call will be routed by the route. If this parameter is null, it means caller number can be any

	number.
Callee Username	The callee number set for matching the route, which supports regular expression. If the callee number of a call matches with this number, the call will be routed by the route. If this parameter is null, it means callee number can be any number.
Time Profile	The profile of time during which the route can be used; If this parameter is null, it means the route can be used at anytime. Please go to **Service -> Time Profile** to get more details
Caller SIP URL	If the 'SIP URL' field of the 'FROM' header of a request message sent by a caller number matches with the value configured here, the call will be routed by the route. If this parameter is null, it means the SIP URL from caller can be any.
Callee SIP URL	If the 'SIP URL' field of the 'FROM' header of a request message sent by a callee number matches with the value configured here, the call will be routed by the route. If this parameter is null, it means the SIP URL from callee can be any.
Source	The source of the call routed by the route. If the source of a call is access network or access SIP trunk, the destination can only be core SIP trunk;

	If the source of a call is core SIP trunk, the destination can be access network or access SIP trunk.
SIP Methods	The SIP method(s) supported by the route. If this parameter is null, it means SIP methods can be any.
Destination	The destination of the call routed by the route. If the destination of a call is access network or access SIP trunk, the source can only be core SIP trunk; If the destination of a call is core SIP trunk, the source can be access network or access SIP trunk.
Request URI	Set the request URI for this route
The source of ring back tone	Configure the source of ring back tone, you can choose remote, local or suit
Destination	The specific SIP truck where a call will be routed
Outbound Manipulation	Configure the source of ring back tone, you can choose Number Manipulation, Number pool or null
SIP Header Passthrough	If it is on, the SIP header of a call routed by the route will be manipulated according to the configured manipulation rule; The parameter is off by default. For manipulation rule, Please go to **Service -> SIP Header Passthrough** to get more details
request-uri Username	Configure the source of the ' request-uri

	Usename ' , You can select values from the configuration items
request-uri IP Addr.	Configure the source of the ' request-uri IP Addr. ' , You can select values from the configuration items
to Username	Configure the source of ' to Username ' , You can select values from the configuration items
to IP Addr.	Configure the source of ' IP Addr. ' , You can select values from the configuration items
to Username Displayed	Configure the source of ' to Username Displayed ' , You can select values from the configuration items
from Username	Configure the source of ' from Username ' , You can select values from the configuration items
from IP Addr.	Configure the source of ' from IP Addr. ' , You can select values from the configuration items
from Username Displayed	Configure the source of 'from Username Displayed' , You can select values from the configuration items

Notes:

Caller number or called number can also be manipulated when a call comes into an access network, access SIP trunk or core SIP trunk. In this section, number is manipulated after a call has finished choosing a route.

3.4.5 Media Detection

On the **Service->Media Detection** page, you can choose to enable/disable ‘Use called to match sessions’ and ‘RTP Detection’ . If ‘RTP Detection’ is enabled, the SBC8000 device will monitor the RTP packets of each call and will disconnect the call after it finds that no RTP packets are sent or received during the detection time.

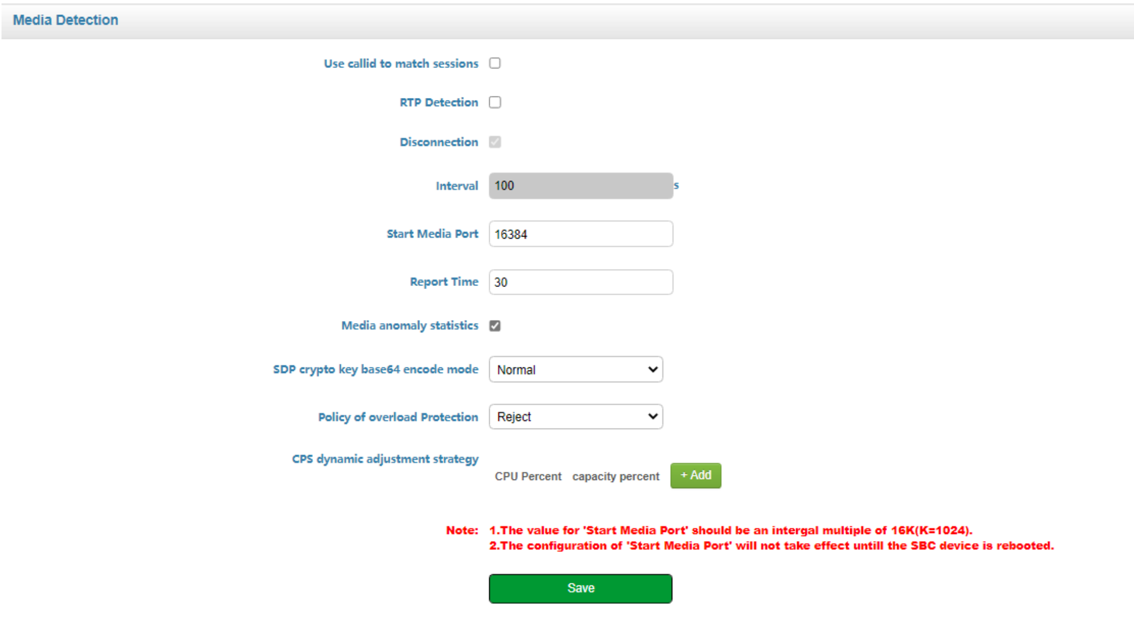


Figure 3-4-6 Media Detection

Table 3-4-6 Media Detection

Use callid to match sessions	After it is enabled, The session standard matches only the Call-id, From and To tags, not the caller and callee number
RTP Detection	RTP Detection can end a call when the voice is single or double down. After it is enabled, You need to configure Disconnection and Interval
Start Media Port	The Start Media Port for all calls is larger than this value and the default is 16384.

	1. The value for 'Start Media Port' should be an intergal multiple of 16K(K=1024). 2. The configuration of 'Start Media Port' will not take effect untill the SBC device is rebooted.
Report Time	The report time of RTP packet
Media anomaly statistics	Alarm reporting in case of media anomaly
SDP crypto key base64 encode mode	Configure SDP crypto key base64 encode mode, Normal or Padding can be selected
Policy of overload Protection	Configure Policy of overload Protection, Reject, Drop or None can be selected
CPS dynamic adjustment strategy	Adjust the system CPS according to the system CPU

3.4.6 CDR

On the **Service CDR** page, the CDR server defaults to 'Disabled', and you need to enable it to do corresponding configurations.

Figure 3-4-7 Configure CDR Server

Table 3-4-7 CDR Server

Name	The name of the CDR server. It cannot be modified after the CDR server has been successfully added
Description	The description of the CDR server
Interface	The interface through which the CDR server receives CDRs
Format	The coded format of CDRs, which supports SYSLOG and JSON
IP Address	The IP address of the CDR server
Port	The SIP port through which the CDR server receives CDRs
Transport	The transport protocol adopted to transport CDRs, which can be UDP or TCP
Attribute	CDR' s specific attributes, check the box to enable

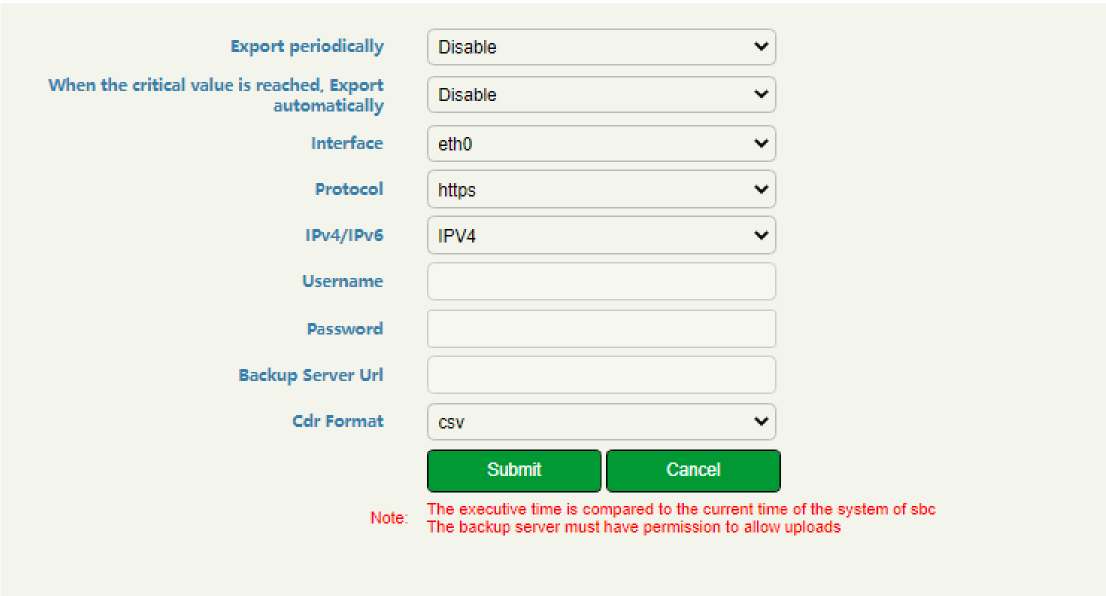


Figure 3-4-8 Local CDRs Exported automatically

Table 3-4-8 Local CDRs Exported automatically

Export periodically	It is disabled by default. When it is enabled, CDRs will be automatically exported at the set time
When the critical value is reached, Export automatically	It is disabled by default. When it is enabled and the critical value is reached, CDRs will be automatically exported to the backup server URL
Interface	The Network Interface of exporting CDRs
Protocol	The protocol adopted to transport CDRs, which only supports https
IPv4/IPv6	The network protocol to be used, whether IPV4 or IPV6
Username	The Username of backup server
Password	The Password of backup server
Backup Server Url	The URL of backup server
Cdr Format	The format of the exported CDRs. The default is txt format. CSV and TXT two formats can be selected

Notes:

1. The executive time is compared to the current time of the system of SBC
2. The backup server must have permission to allow uploads

3.4.7 Codec Profile

The system of SBC8000 supports codecs including G.729, G.723, PCMU, PCMA, ILBC_13K, ILBC_15K, OPUS, AMR and AMR_WB and so on. You can group these codecs and adjust their priority according to your routing needs.

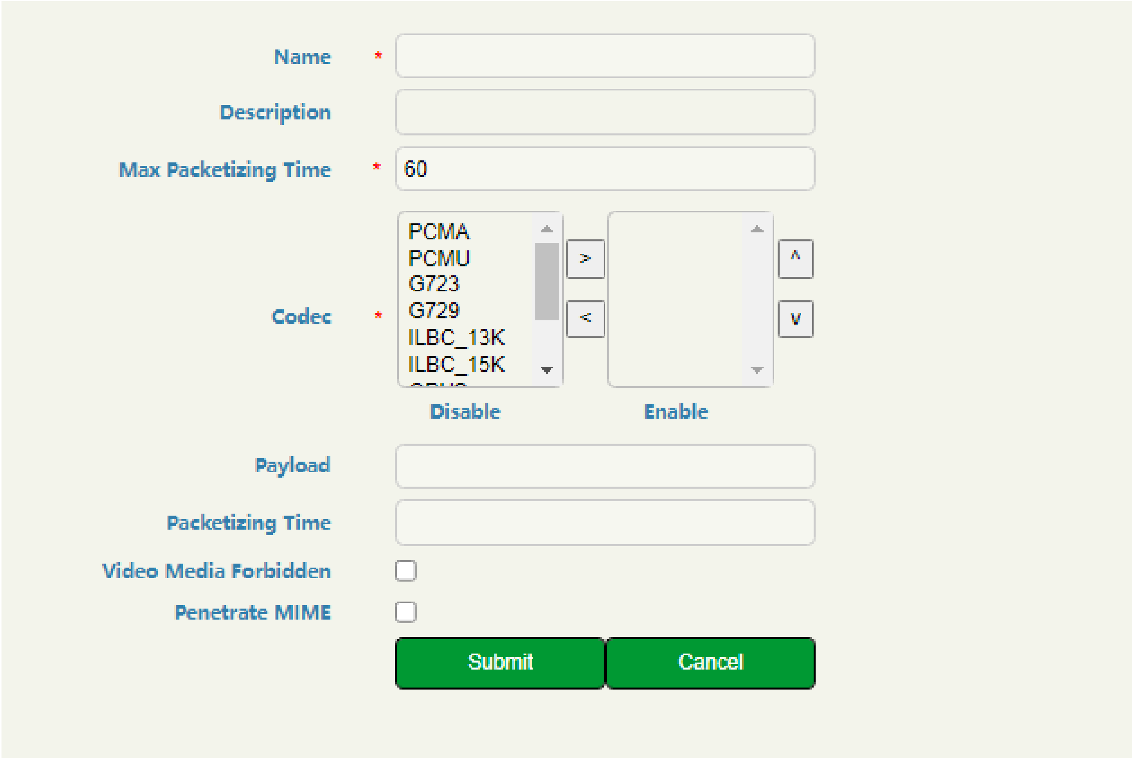


Figure 3-4-9 Codec Profile

Table 3-4-9 Codec Profile

Name	The name of the codec group. It cannot be modified after the codec group has been added successfully
Description	The description of the codec group
Max Packetizing Time	The maximum packetizing time that the codec group supports
Codec	SBC8000 supports codecs including G.729, G.723, PCMU, PCMA, ILBC_13K, ILBC_15K, OPUS, AMR and AMR_WB
Payload	The codec value of each codec, which cannot be modified

Packetizing Time	The default packetizing time of each codec, which cannot be modified
Video Media Forbidden	Do not pass through the video media after checking the box
Penetrate MIME	The SBC will penetrate MIME after checking the box

Notes:

There is a default codec group on the page. This codec group includes all the codecs by default. It can be modified but cannot be deleted.

3.4.8 TLS Configuration

On this page, you can configure the version of TLS protocol and Cipher suites. Only the default configuration can be modified, no new configuration can be added.

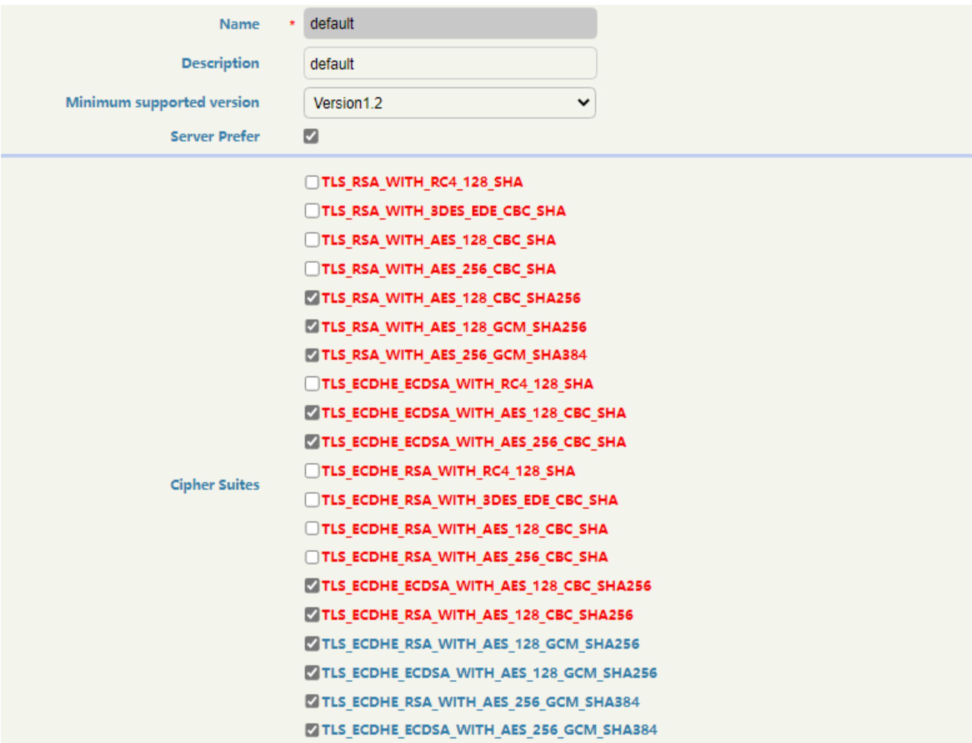


Figure 3-4-10 TLS Configuration

Table 3-4-10 TLS Configuration

Name	The name of the TLS configuration The default name is default and cannot be modified
Description	Description of the TLS configuration. Users can describe the use of this TLS in more details.
Minimum supported version	The minimum version of the TLS protocol supported by the system of SBC8000
Server Prefer	Select the server's TLS protocol version and Cipher suites in priority after checking the box
Cipher Suites	After checking the box, the Cipher suites will be used by the system

Note:

The marked red encryption kit has potential security risks, please use it with caution.

3.4.9 Active And Standby

On this page, you can configure the parameters related to Active And Standby, BFD Detect，Network Port Detection and Switching Rules.

3.4.9.1 Active And Standby Configuration

Here you can configure the parameters related to Active And Standby.

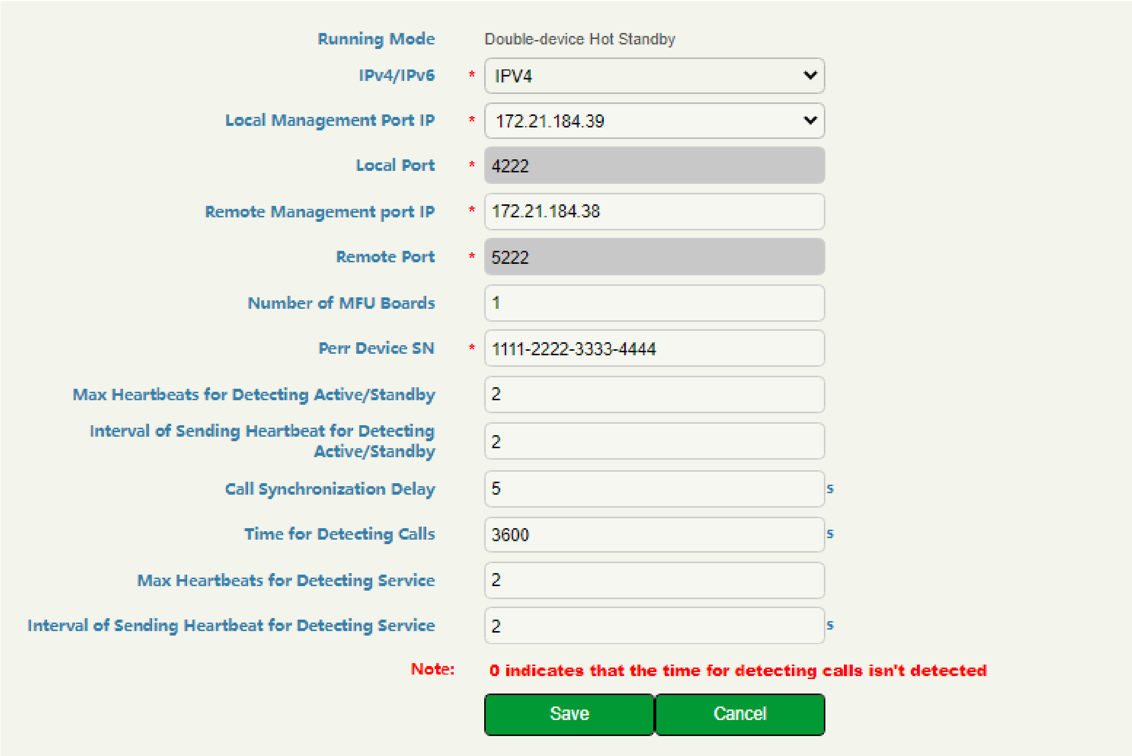


Figure 3-4-11 Active And Standby Configuration

Table 3-4-11 Active And Standby Configuration

IPv4/IPv6	The network protocol to be used, whether IPV4 or IPV6
Local Management Port IP	The IP address of the Local Management Port
Local Port	Local port for Active/Standby Heartbeats Detection and Transmission
Remote Management port IP	The IP address of the Remote Management Port
Remote Port	Remote port for Active/Standby Heartbeats Detection and Transmission
Number of MFU Boards	You can select the number of MFU Boards to be monitored

Perr Device SN	Device serial number of the remote SBC
Max Heartbeats for Detecting Active/Standby	The maximum number of Heartbeats for Active/Standby detection
Interval of Sending Heartbeat for Detecting Active/Standby	The interval of Sending Heartbeat for Detecting Active/Standby
Call Synchronization Delay	The delay time for call synchronization
Time for Detecting Calls	The duration of call detection. 0 indicates that the time for detecting calls isn't detected
Max Heartbeats for Detecting Service	The maximum number of Heartbeats for Detecting Service
Interval of Sending Heartbeat for Detecting Service	The interval of Sending Heartbeat for Detecting Service

3.4.9.2 BFD Detect

On this page, you can configure the related parameters for BFD detection.

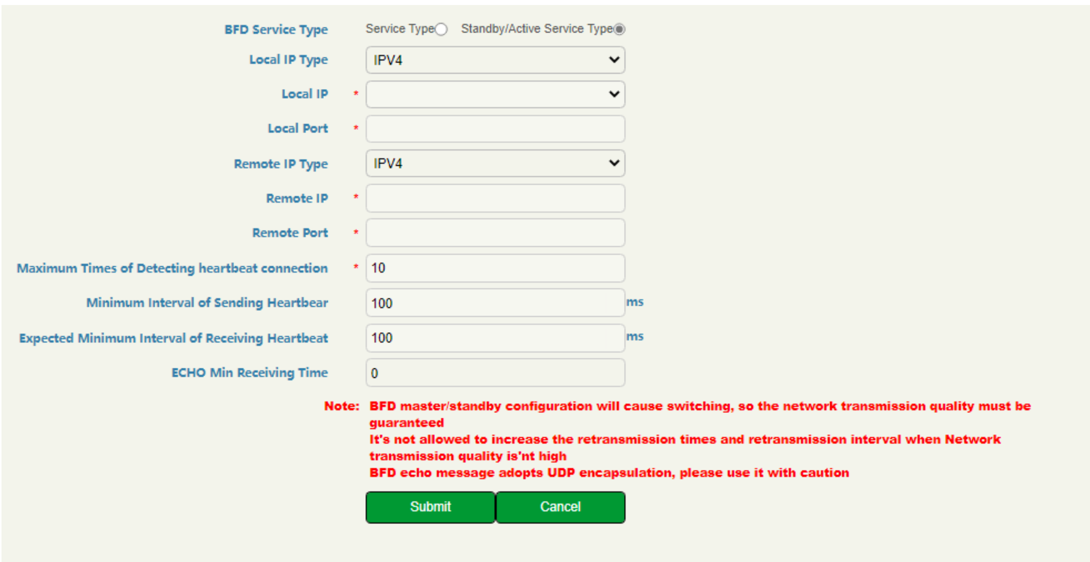


Figure 3-4-12 BFD Detect

Table 3-4-12 BFD Detect

BFD Service Type	You can select Service Type or Standby/Active Service Type. It cannot be modified after the BFD Service Type has been saved successfully
Local IP Type	The network protocol to be used, whether IPV4 or IPV6
Local IP	You can select the Local IP Address of BFD Detection
Local Port	You can select the Local Port of BFD Detection
Remote IP Type	Select the IP address type of the remote SBC, which can be IPv4 or ipv6
Remote IP	Configure the IP address of the remote SBC
Remote Port	Configure the port for BFD detection of remote SBC.
Maximum Times of Detecting heartbeat connection	Maximum number of BFD detections. Status Failure is displayed after this number is beyond.
Minimum Interval of Sending Heartbear	Minimum transmit interval for BFD detection
Expected Minimum Interval of Receiving Heartbeat	Expected Minimum Interval of Receiving Heartbeat
ECHO Min Receiving Time	Minimum reception interval for ECHO

Note:

1. BFD master/standby configuration will cause switching, so the network transmission quality must be guaranteed

2. It's not allowed to increase the retransmission times and retransmission interval when network transmission quality isn't high

3. BFD echo message adopts UDP encapsulation, please use it with caution

3.4.9.3 Network Port Detection

On this page, you can select the network port that requires network port detection, and after selecting it, the information such as the IP address will be displayed.

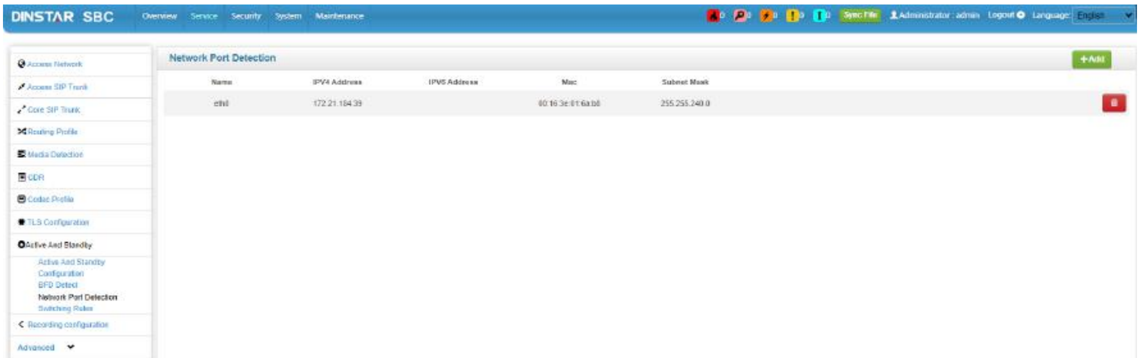


Figure 3-4-13 Network Port Detection

Table 3-4-13 Network Port Detection

Name	The name of Network Port
IPV4 Address	The IPV4 Address of Network Port
IPV6 Address	The IPV6 Address of Network Port
Mac	The Mac Address of Network Port
Subnet Mask	The Subnet Mask of Network Port

3.4.9.4 Switching Rules

On this page, you can configure the Switching Rules.

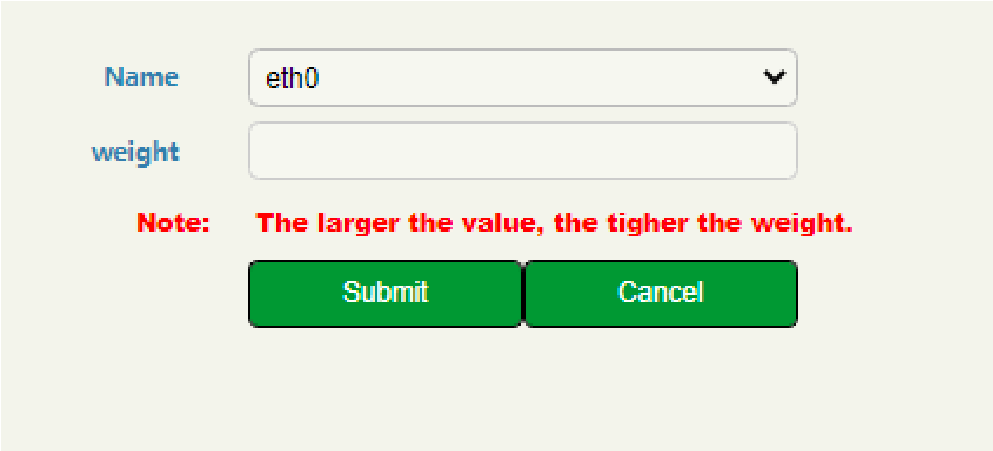


Figure 3-4-14 Switching Rules

Table 3-4-14 Switching Rules

Name	Select the network port to detect
weight	Configure the weight of this Switching Rule. The larger the value, the tigher the weight.

3.4.10 Recording Configuration

3.4.10.1 SipRec configuration

The SBC8000 supports call recording through siprec server.

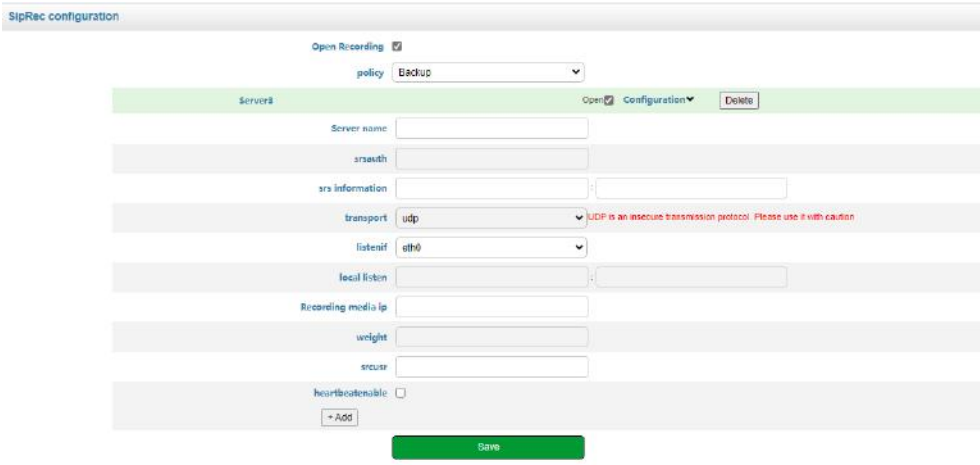


Figure 3-4-15 SipRec configuration

Table 3-4-15 SipRec configuration

Policy	Server Policy when configuring multiple recording servers: Backup/load balance
Server name	The name of Recording Server
srsauth	The secret key for server authentication
srs information	The recording IP address of the server
transport	The communication protocol for interacting with the server, which only supports UDP currently
listenif	The communication port that the SBC listens to
local listen	The listening IP and port for SBC recording signal
Recording media ip	The listening IP for SBC recording media
weight	When there are multiple servers, you can set weight value for each server
srcusr	The username used for Sip recording calls
heartbeatenable	When it is enabled, SBC automatically sends heartbeat

	messages to the server to confirm that the server is online or the connection with the server is normal. You need to configure maxcount (the number of heartbeat timeouts), period(heartbeat detection period), and isvalidateresp (only match 200 as valid response)

3.4.11 Number Profile

On the **Service -> Number Profile** page, you can set a prefix for calling numbers or called numbers. When the prefix of a calling number or a called number matches the set prefix, the call will be passed to choose a route. Number profile does not support 'Regular Expression' currently.

Click 

, and you can add a number profile.

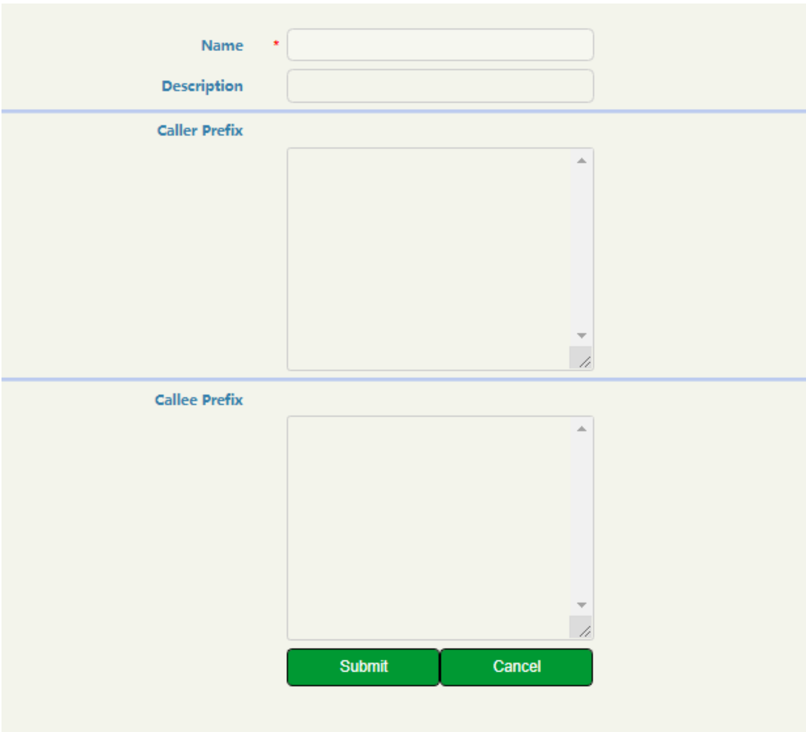


Figure 3-4-16 Add Number Profile

Table 3-4-16 Number Profile

Name	The name of the number profile. It cannot be modified after the number profile is added successfully
Description	The description of the number profile
Caller Prefix	The prefix set for caller numbers. It does not support **regular expression.** When the prefix of a caller number matches the set prefix, the call will be passed to choose a specific route.
Callee Prefix	The prefix set for callee numbers. It does not support **regular expression.** When the prefix of a callee number matches the set prefix, the call will be passed to choose a specific route.

3.4.12 Black & White List

On the **Service -> Black & White List** page, you can choose to put calling numbers on black list or white list. If a number is put on black list and the black list is linked to an access network, an access SIP trunk or a core SIP trunk, the SBC8000 will refuse the calls and registration requests from this number.

If a number is put on whitelist and the white list is adopted, the SBC8000 will accept the calls and registration requests from this number.

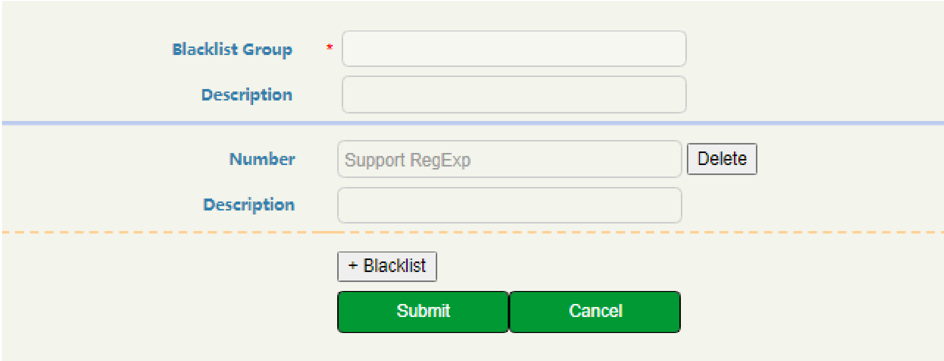


Figure 3-4-17 Blacklist

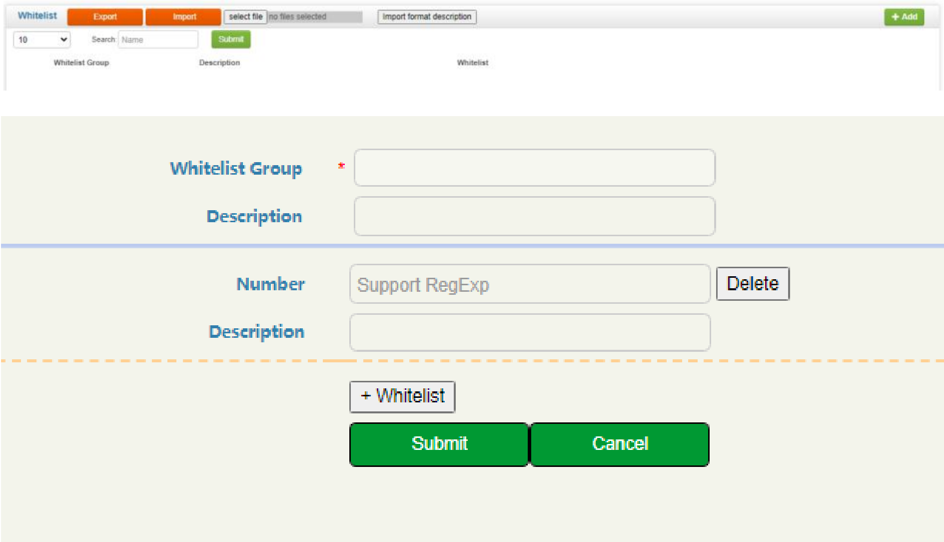


Figure 3-4-18 Whitelist

Table 3-4-17 Blacklist & Whitelist

Blacklist Group	The name of the blacklist. It cannot be modified after the blacklist group is added successfully
Whitelist Group	The name of the whitelist. It cannot be modified after the whitelist group is added successfully
Description	The description of the blacklist/ whitelist group
Number	The calling number(s) that is (are) put on blacklist/ whitelist. It does not support **regular expression.**
Description	The description of a specific blacklist/ whitelist

3.4.13 Number Manipulation

Number manipulation refers to the change of a called number or a caller number during calling process when the called number or the caller number matches the preset rules.

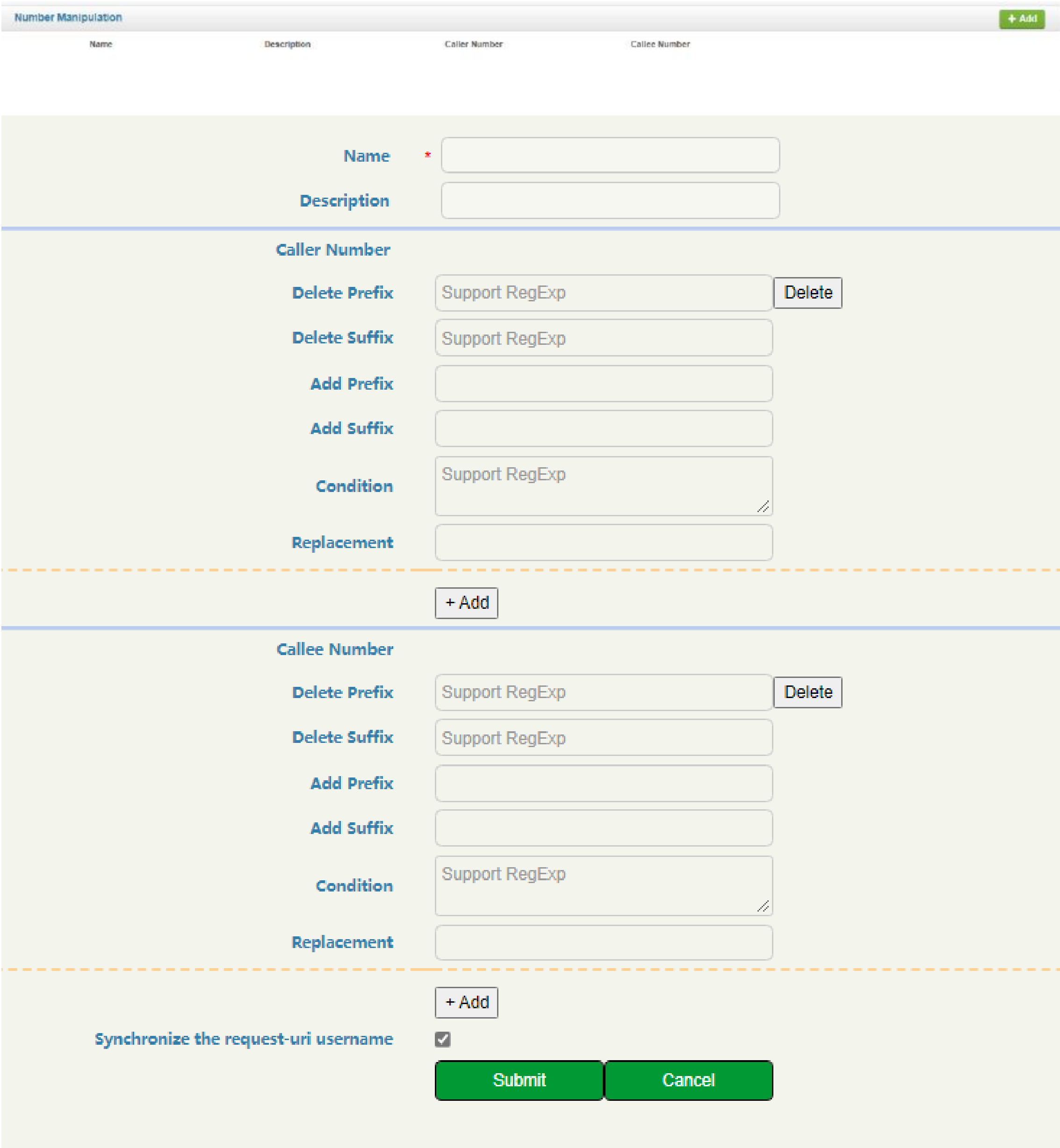


Figure 3-4-19 Configure Number Manipulation Rule

Table 3-4-18 Number Manipulation Rule

Name	The name of this manipulation rule. It cannot be modified after the manipulation rule has been added successfully
Description	The description of this manipulation rule
Delete Prefix	The prefix that will be deleted after it matches a caller/callee number. For example, if the prefix is set as 678 and the caller number is 67890000, then the caller number will be changed into 9000; The prefix supports regular expression; Multiple prefixes can be set for one manipulation rule.
Delete Suffix	The suffix that will be deleted after it matches a caller/callee number. For example, if the suffix is set as 123 and the caller number is 8000123, then the caller number will be changed into 8000; The suffix supports regular expression; Multiple suffixes can be set for one manipulation rule.
Add Prefix	The prefix added to the caller/callee number. For example, if the prefix is set as 678 and the caller number is 9000, then the caller number will be changed into 6789000 after the manipulation rule is matched; The prefix does not support regular expression;

Add Suffix	The suffix added to the caller/callee number For example, if the suffix is set as 678 and the caller number is 9000, then the caller number will be changed into 9000678 after the manipulation rule is matched; The suffix does not support regular expression;
Condition	The condition supports regular expression. If a caller/callee number can match one of the rules set in the 'Condition' parameter, the original number will be changed into the one set in the 'Replaced By' parameter.
Replacement	If a caller/callee number can match one of the rules set in the 'Condition' parameter, the original number will be changed into the one set in the 'Replaced By' parameter. The value of the 'Replaced By' parameter does not support regular expression.
Synchronize the request-uri username	After checking the box, the request-uri user name will be changed synchronously

Notes:

1. During number manipulation, 'Delete Prefix' and 'Delete Suffix' are carried out first, followed by 'Add Prefix' and 'Add Suffix'. If 'Condition' is also set, SBC8000 will match the condition based on the result of the abovementioned rules.

2. If a number manipulation rule is used on the **Service- > Access Network** page, the **Service -> Access SIP Trunk** page or the **Service -> Core SIP Trunk** page, it means the caller/callee number will be manipulated before the

call chooses a route;

3. If a number manipulation rule is used on the **Service Routing Profiles** page, it means the caller/callee number will be manipulated after the call has chosen a specific route.

3.4.14 Number Pool

On the **Service -> Number Pool** page, you can set a number pool. If the number pool is used on the **Service Routing Profiles** page, the caller/callee number will be randomly replaced by a number from the pool.

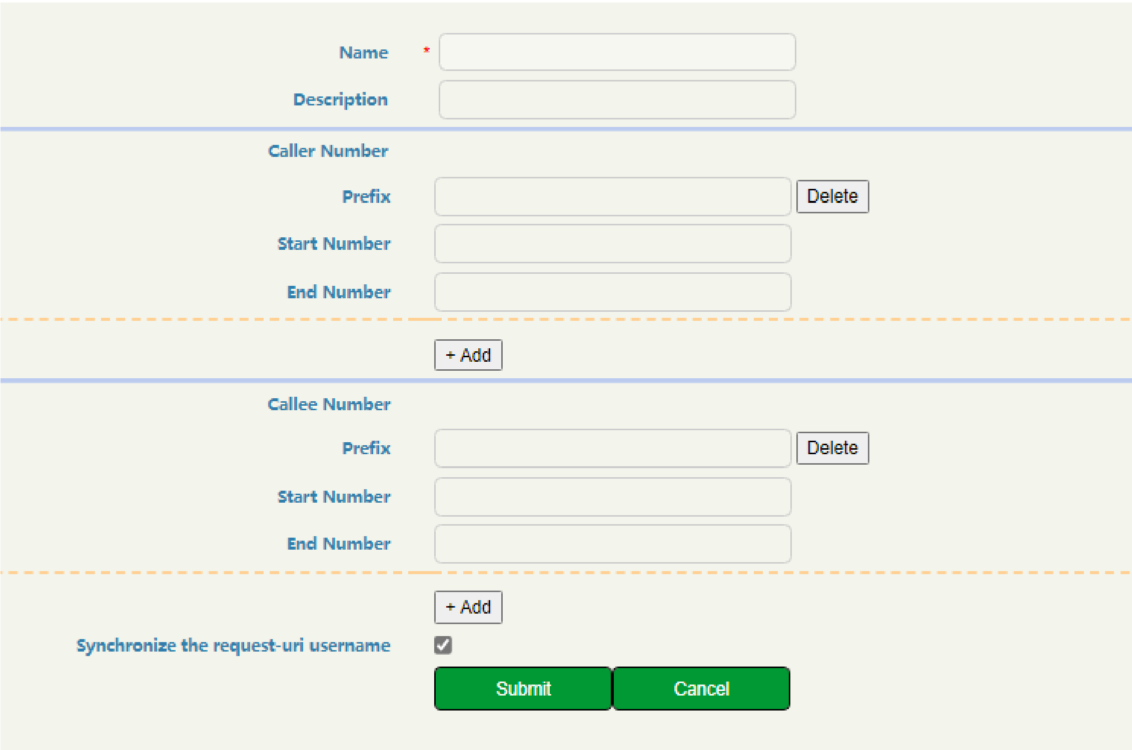


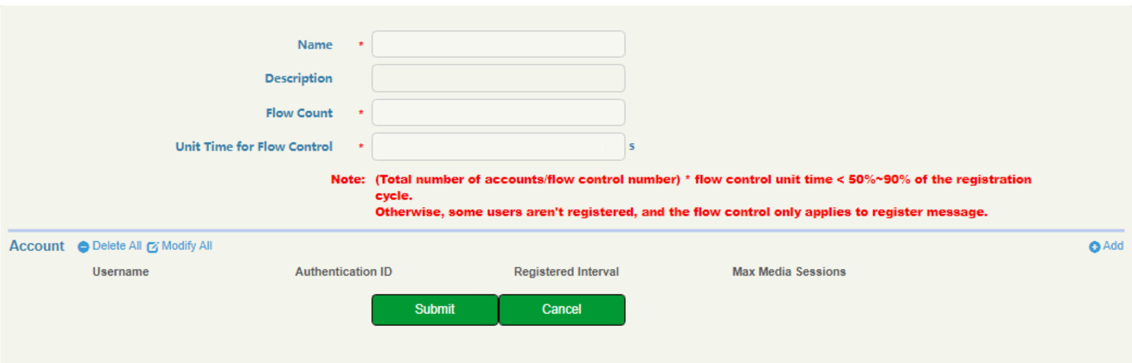
Figure 3-4-20 Configure Number Pool

Table 3-4-19 Number Pool

Name	The name of this number pool. It cannot be modified after the number pool has been added successfully
Description	The description of this manipulation rule
Caller/Callee Number	**Prefix**: If the prefix here is matched with a caller/callee number, the caller/callee number will be randomly replaced by a number from the pool; **Start Number**: The starting number of the number pool **End Number**: The ending number of the number pool
Synchronize the request-uri username	After checking the box, the request-uri user name will be changed synchronously

3.4.15 SIP Account

On this page, you can configure the account information that SBC registers to the server. The SBC supports importing and exporting account information.



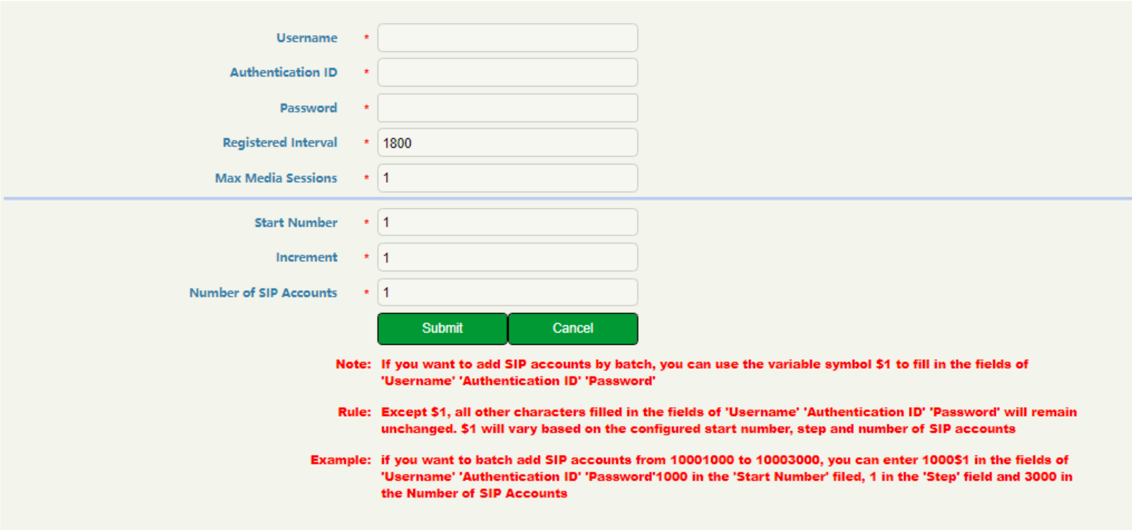


Figure 3-4-21 Configure SIP Account

Table 3-4-20 SIP Account

Name	The name of this SIP Account. It cannot be modified after the SIP Account has been added successfully
Description	The description of the sip account
Flow Count	Number of registrations during the unit time
Unit Time for Flow Control	Minimum registration unit time for flow controls
Username	Username for registered SIP account
Authentication ID	The authentication ID of the registered account. It must be consistent with the sip server, otherwise it will not be registered.
Password	Authentication password for registered accounts
Registered Interval	If the registration is not successful during this period, the registration will be initiated again after this time period.

Max Media Sessions	Maximum number of concurrent calls for this account
Start Number	User name, authentication ID, password options support rule adaptation. The starting value of variable character $1
Increment	Increment of variable character $1
Number of SIP Accounts	Total number of accounts with variable character $1

Note:

(Total number of accounts/flow control number) * flow control unit time < 50%~90% of the registration cycle. Otherwise, some users aren't registered, and the flow control only applies to register message.

3.4.16 Time Profile

On the **Service Time Profile** page, you can set a time period for calls to choose routes. When a call is initiated and the time meets a time set in the Time Profile, the call will be triggered with a corresponding route. If a call is initiated without matching any time set in the profile, the call cannot be routed and rejected.

Click 

, and you can add a time profile.

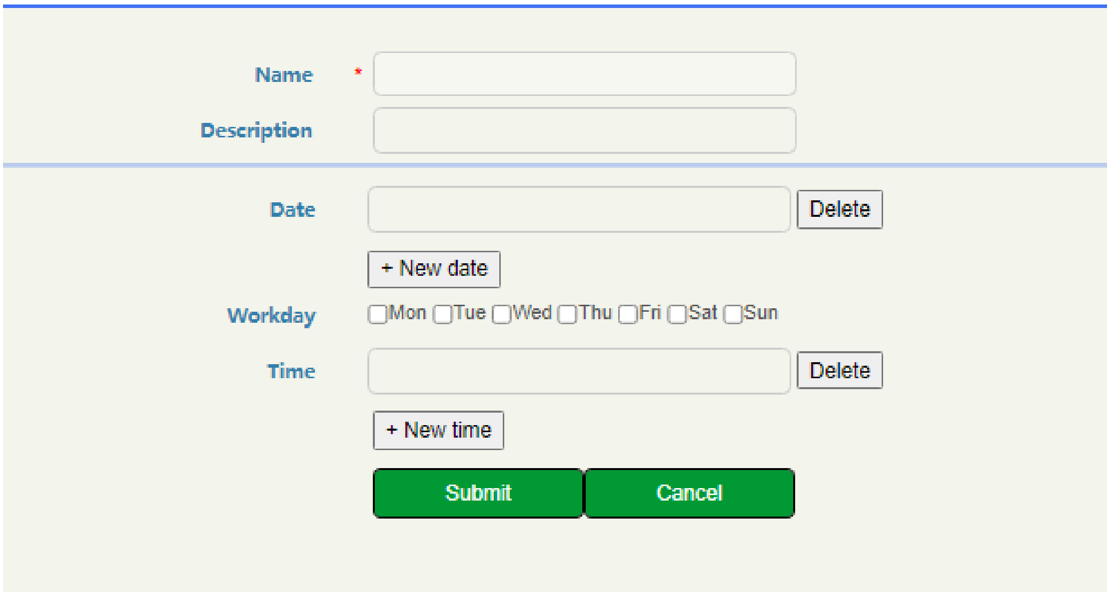


Figure 3-4-22 Add Time Profile

Table 3-4-21 Time Profile

Name	The name of the time profile. It cannot be modified after the time profile is added successfully
Description	The description of the time profile
Date	Configure the starting date and ending date of a period; You are allowed to configure multiple periods
Workday	Choose one or more working days (from Monday to Sunday)
Time	Choose the starting time and ending time of a day You are allowed to configure multiple time periods

3.4.17 Rate Limit

On the **Service -> Rate Limit** page, you can configure the maximum registrations per second (RPS), maximum calls per second (CPS) and maximum concurrent calls for access network, access SIP trunk and core SIP trunk.

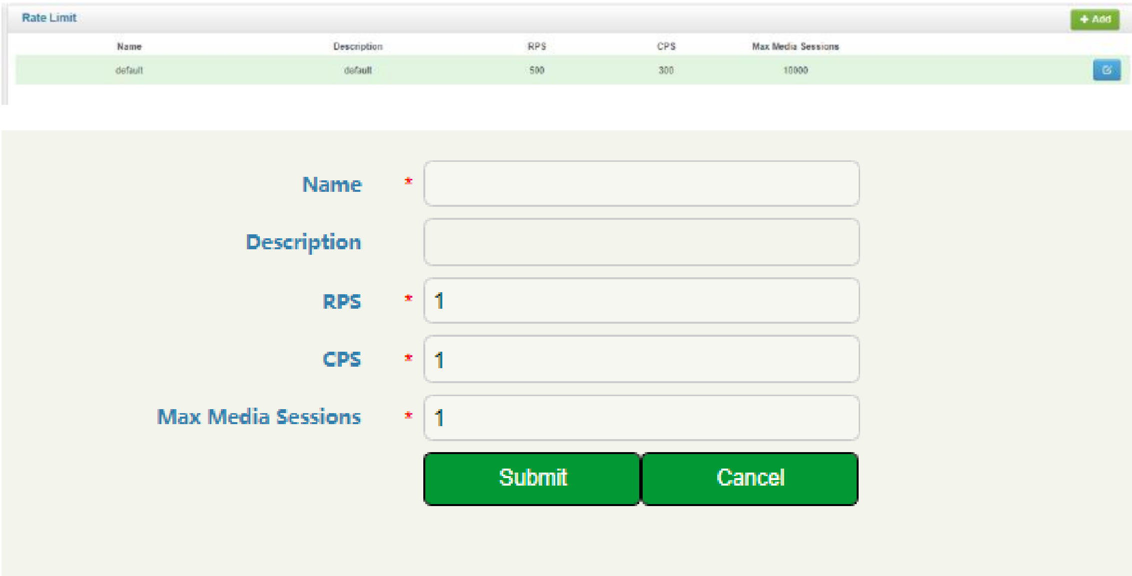


Figure 3-4-23 Add Rate Limit

Table 3-4-22 Rate Limit

Name	The name of the rate limit rule. It cannot be modified after the rate limit rule is added successfully
Description	The description of the rate limit rule
RPS	The maximum number of registrations that is allowed per second
CPS	The maximum number of calls that is allowed per second
Max Media Sessions	The maximum number of concurrent calls that is allowed

Notes:

1. There is a default rate limit rule on the page. Its RPS, CPS and maximum number of concurrent calls are defined by License.

2. The RPS, CPS and maximum concurrent calls configured in other rate limit rules cannot be greater than those of default rule.

3.4.18 SIP Header Manipulation

When the SIP headers of the messages related to calls passing through access network, access SIP trunk and core SIP trunk are not consistent with those required, you need to set rules to manipulate original SIP headers.

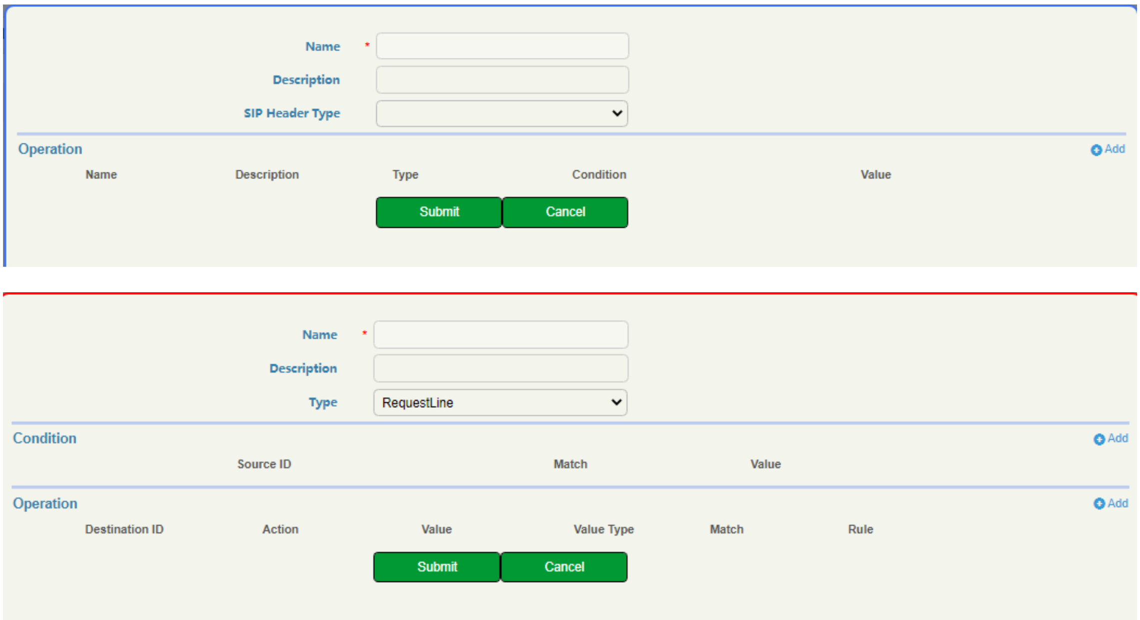


Figure 3-4-24 Configure SIP Header Manipulation Rule

Table 3-4-23 SIP Header Manipulation

Name	The name of the SIP header manipulation rule. It cannot be modified after the SIP header manipulation rule has been added successfully
Description	The description of the SIP header manipulation rule
SIP Header Type	Request: The manipulation rule is only applied to SIP request messages; Response: The manipulation rule is only applied to SIP response messages; List: The manipulation rule is only applied to those SIP request and response messages that are selected
Operation	The operation rule will be applied when the set condition is met. For example, when the set value meets the source ID in Request Line, the actions(add, modify or remove) will be conducted on the destination ID. **Name**: the name of the operation rule. **Description**: the description of the operation rule. **Type**: the content type where the operation rule will be applied. Request-line: the content of the request line of SIP message. Status-line: the content of the status line of SIP message. Header: the content of the header of SIP message. **Condition**: the set condition for the operation rule.

	When the set value matches the source ID, the operation rule will be activated. **Source ID**: the original content of SIP message, it can be any parameter included in SIP message. **Match**: equal when the source ID is equal to the set value, the operation rule is activate. Regex when the source ID matches the set regular expression, the operation rule will be activated. **Value**: the value set to match the source ID. **Destination ID**: the designated header to be modified. **Action**: The actions (add, modify or remove) to manipulate SIP header after the preset conditions is matched. **Value Type**: Token In the 'Value' field, the content with $ is the content which is from the designated header of original SIP message. **Value**: In the Token and Regex value types, the value of the specified field of the original message is referenced with $.

Note:

1. When you quote the value of the original message with $, you must refer to the configuration method of the target identifier, for example, to quote the value of user in the to field of the original message, you should enter $to.$.uri$.user.

2. All values quoted with $ are the values of the original message (SIP message before transformation), not the manipulated values (e.g. number

Manipulation, SIP header Manipulation, etc.).

3. Each SIP header field parameter has a specification, and users are suggested to modify or match it strictly according to the parameter rules.

3.4.19 SIP Header Passthrough

On the **Service -> SIP Header Passthrough** page, you can configure one or more 'SIP Header Passthrough' profiles. If the profiles are used on the **Service -> Routing Profile** page, the designated extension fields of SIP messages of a specific route will be passed through.

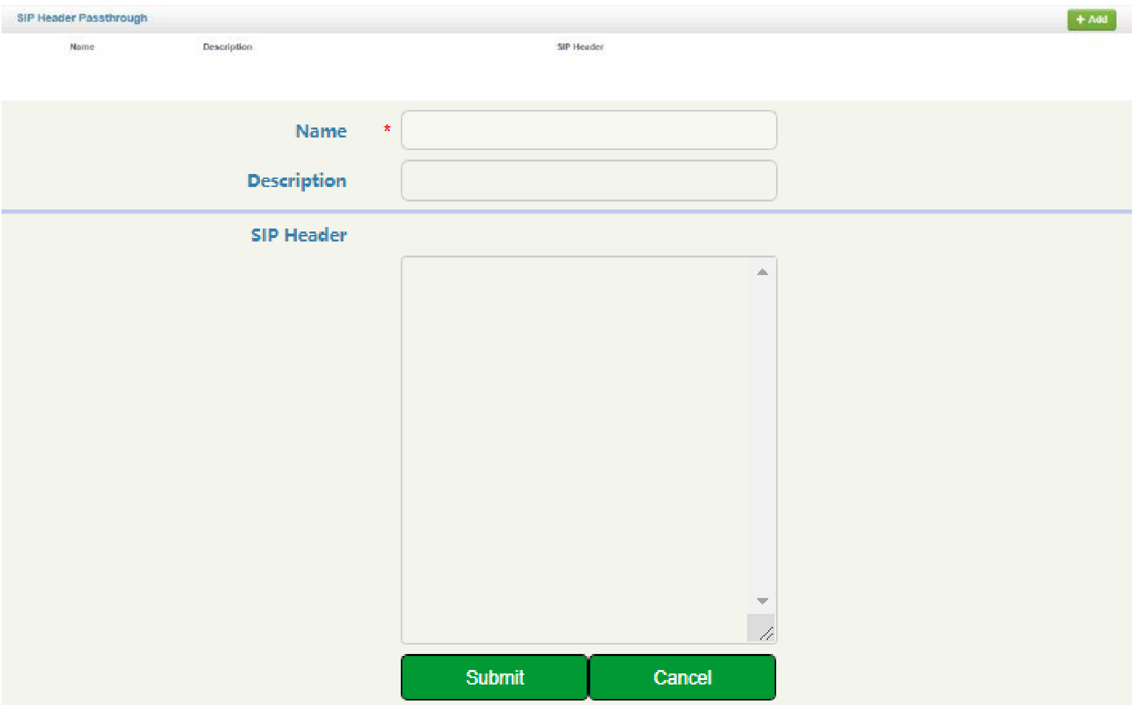


Figure 3-4-25 SIP Header Passthrough

Table 3-4-24 SIP Header Passthrough

Name	The name of the 'SIP header passthrough' profile. It cannot be modified after the 'SIP header pass' profile has been added successfully
Description	The description of the 'SIP header passthrough' profile
SIP Header	The SIP headers that are passed through. A SIP header in a row, case-sensitive, without any extra punctuation marks

Notes:

1. The 'Allow' and 'Supported' SIP headers can only be passed through during registration. That is to say, they cannot be passed through during calling. Please think carefully before passing through these two SIP headers, as they might conflict with the configurations of SBC8000.
2. The following SIP heads are not allowed to be passed through:

    Network, To, From, Contact, Cseq, Max-Forwards, Content-Length, Content-Type, Via, Require, Proxy-Require, Unsupported, Authorization, Proxy-Authorization, Www-Authenticate, Proxy-Authenticate, Accept, Route, Record-Route, Refer-To, Referred-By, Auto-Defined.

3.4.20 Quality Monitoring

Quality Monitoring is used to monitor the quality of the network between local and remote, and to process subsequent communications when the configured standards are reached.

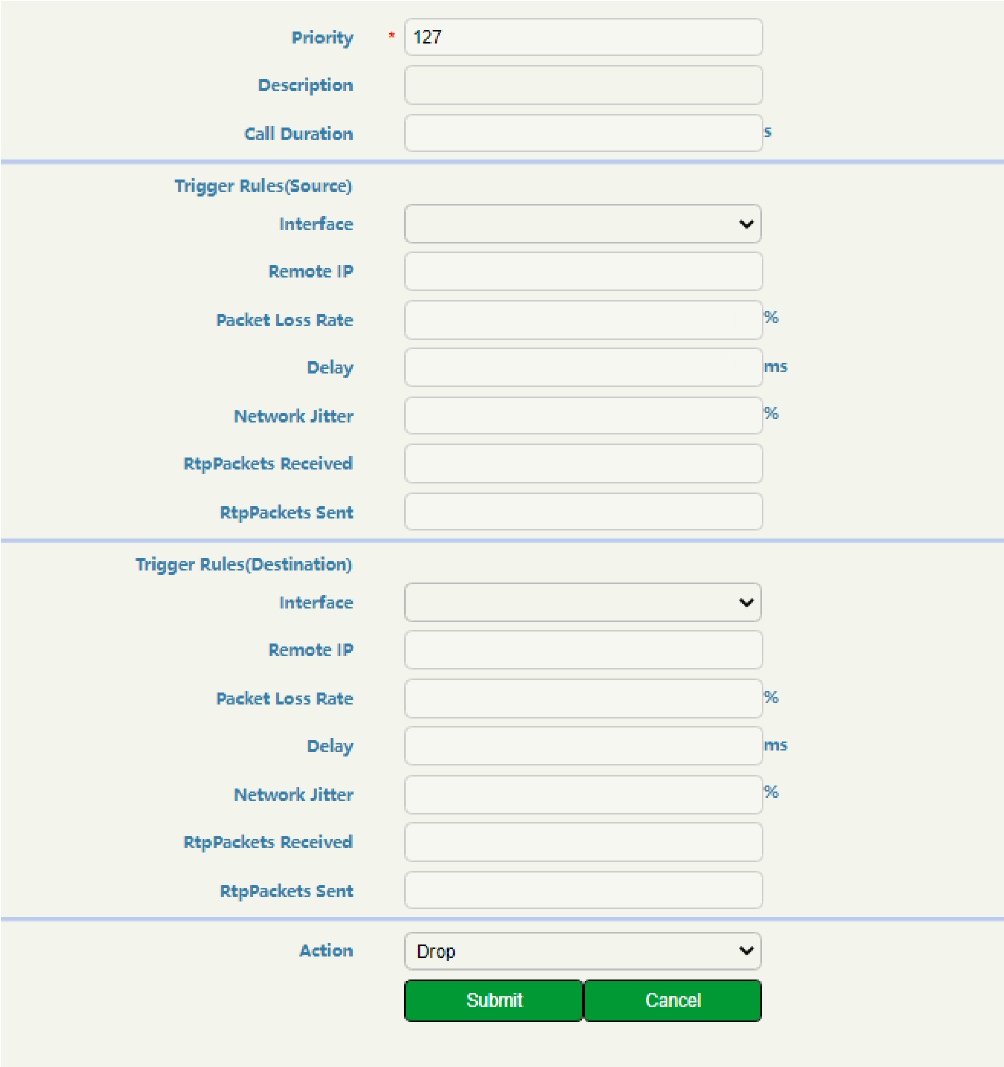


Figure 3-4-26 Quality Monitoring

Table 3-4-25 Quality Monitoring

Priority	The priority of passing this quality monitoring after making a call. The higher the number, The higher the priority.
Description	The role and purpose of this quality monitoring, which is set by users
Call Duration	Call duration through this trunk
Interface	Interface of monitored calls

Remote IP	The remote IP address which is connected to the monitoring interface
Packet Loss Rate	The Packet Loss Rate is the rate between the number of lost packets to the total number of packets sent.
Delay	The time that it takes for a message or packet to travel from one end of the network to the other
Network Jitter	Packet Delay Variation (PDV), is a stuttering like effect in signal quality because of inconsistent packet delays in a data transmission
RtpPackets Received/Sent	Number of RTP received/sent packets
Action	The action of the SBC after the trigger condition is reached, including drop,warning and log.

3.4.21 Bandwidth Limit

You can limit the bandwidth of each voice/video call depending on codec.

Figure 3-4-27 Bandwidth Limit

Table 3-4-26 Bandwidth Limit

Name	The name of the Bandwidth Limit . It cannot be modified after the Bandwidth Limit has been added successfully
Description	The function and purpose of this bandwidth limit, which can be set by users.
Audio/Video	The rule will take effect only after it is applied in the Access/Core SIP Trunk, and the audio and video through this Access/Core SIP Trunk will be limited in bandwidth after it is applied.

Note:

1. Under the bandwidth limit strategy, each voice call is pre-allocated with 200 kbps and each video call is pre-allocated with 2 mbps.

3.5 Security

In the **Security** section, you can configure the system security strategies, anti-attack strategies and access control strategies.

3.5.1 Access Control

On the **Security -> Access Control** page, you can configure the access ports for Web.

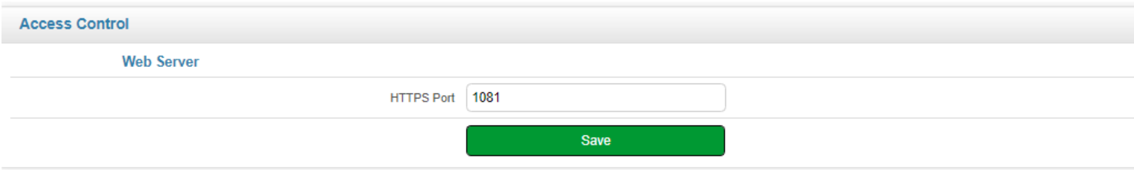


Figure 3-5-1 Access Control

Table 3-5-1 Access Control

Web Server	HTTPS port: the port used to access the web through the https protocol, the default is 1081. Users can modify it.

3.5.2 Security Policy

3.5.2.1 SIP Security

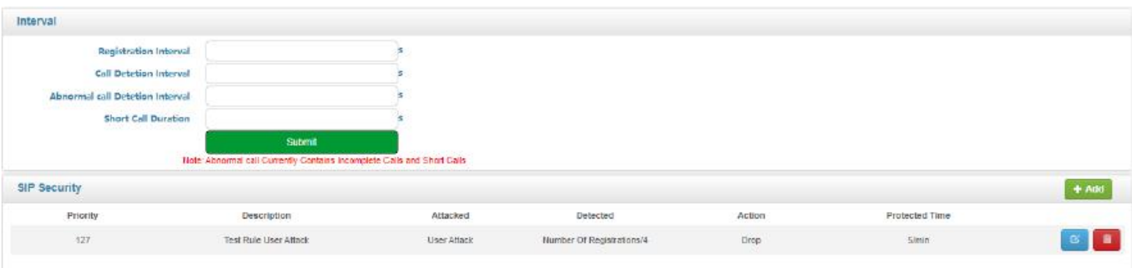


Figure 3-5-2 SIP Security Strategy

Click  to add a strategy to prevent attacks from SIP-based devices. Click

 to delete a strategy, while click  to modify the strategy.

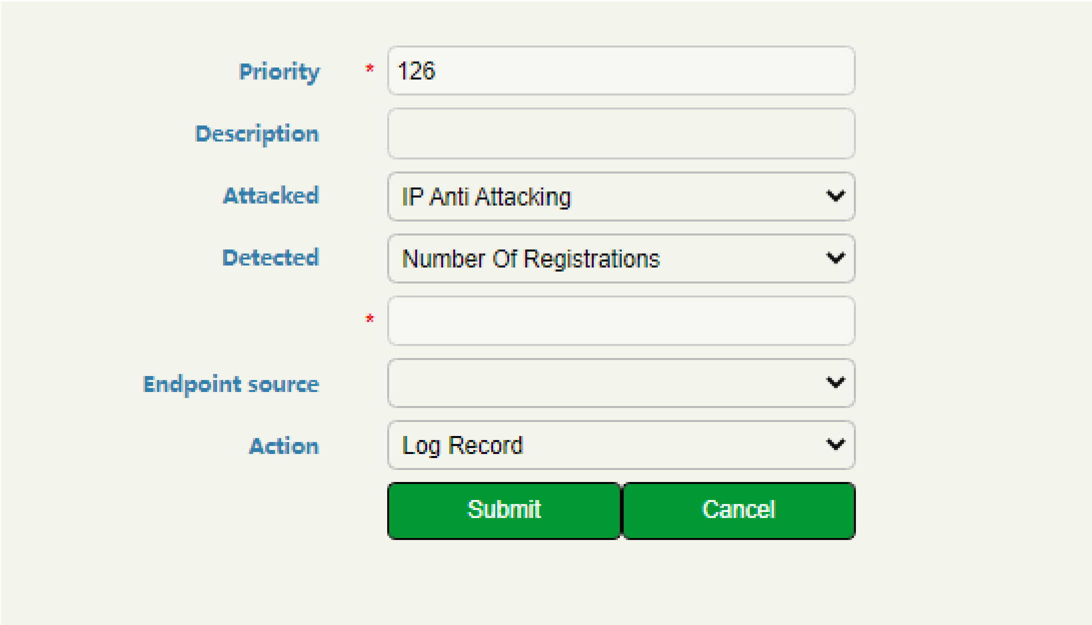


Figure 3-5-3 Add SIP Security Strategy

Table 3-5-2 SIP Security Strategy

Registration Interval	If the configured number of registrations is detected during the registration interval, it is identified as a SIP attack
Call Detetion Interval	If the configured number of calls is detected during the call detetion interval, it is identified as a SIP attack
Abnormal call Detetion Interval	If the configured number of abnormal calls is detected during the abnormal call detetion interval, it is identified as a SIP attack. Abnormal calls include short calls and incomplete calls.
Short Call Duration	Calls that are below the value are identified as short calls

Priority	The lower the value of priority, the higher the priority level
Description	The role and purpose of this SIP anti-attack policy. It can be configured by the users
Attacked	Configure the type of attack object: IP Anti attacking/User attack IP Anti attacking: When the number of SIP messages sent from an IP in the detection period has exceeded the set value, the system will handle the SIP messages sent from that IP based on the action type. User attack: When the number of registration/call (caller) messages sent to the same user and access network listening port during the detection period has exceeded the set value, the system will handle the SIP messages based on the action type for that user.
Detected	Configure the type of detection:Number of Registrations/Number of Calls/Number of Short Calls/Number of Incomplete Calls Number of Registrations: The system will detect the number of REGISTER messages sent from the same IP or user. If the number of times found in the detection period has exceeded the value, the system will handle the REGISTER message based on the action type for that IP or user Number of Calls: The system will detect the number of INVITE messages sent from the same IP or user. If the number of times found in the detection period has

	exceeded the value, the system will handle the INVITE message based on the action type for that IP or user Number of Short Calls: The system will detect the number of short calls sent from the same IP or user. If the number of times found in the detection period has exceeded the value, the system will handle the INVITE message based on the action type for that IP or user Number of Incomplete Calls: The system will detect the number of incomplete calls sent from the same IP or user. If the number of times found in the detection period has exceeded the value, the system will handle the INVITE message based on the action type for that IP or user
Endpoint source	Configure endpoint source for SIP attack detection
Action	Log Record: When this policy is in effect, only this event log is recorded Discard: When this policy is in effect, all messages received by this endpoint will be dropped for the limited time
Protected Time	The time when the SIP anti-attack policy takes effect. A policy needs to be re-evaluated to check if it is effective after the set time.

3.5.3 Web Authentication Configuration

3.5.3.1 Authentication strategy

On this page, you can configure the priority of the Authentication Method, which can be selected from Local Authentication and Radius Authentication.

Figure 3-5-4 Authentication Strategy

Notes:

1. Authentication mode defaults to local authentication
2. When the authentication method does not include local authentication, if the authentication fails, the local authentication will be performed.

3.5.3.2 Tacacs Authentication Configuration

On this page, you can configure the server parameters for tacacs authentication.

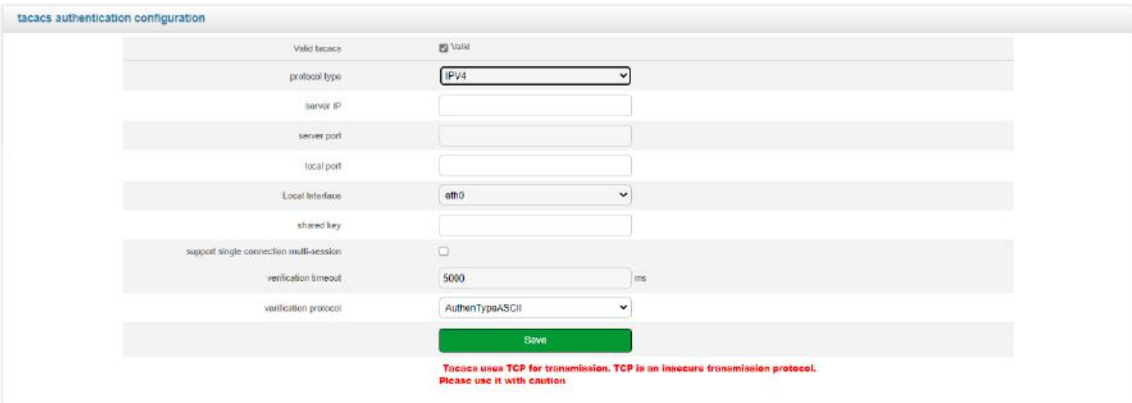


Figure 3-5-5 tacacs authentication configuration

Table 3-5-3 tacacs authentication configuration

protocol type	The type of protocol to interact with the server. You can choose ipv4/ipv6
server IP	The IP address of the Tacacs server
server port	The authentication port of the Tacacs server
local port	The listening port of the tacacs service of the SBC
Local Interface	The physical network interface of the SBC
shared key	The shared key to interact with the tacacs server
support single connection multi-session	The system can support single connection multi-session after you enable it
verification timeout	The timeout period of the Tacacs authentication. The authentication fails after the specified time.
verification protocol	The verification protocol of Tacacs authentication

3.5.3.3 Radius configuration

In this page, you can configure the parameters related to radius authentication and bill.

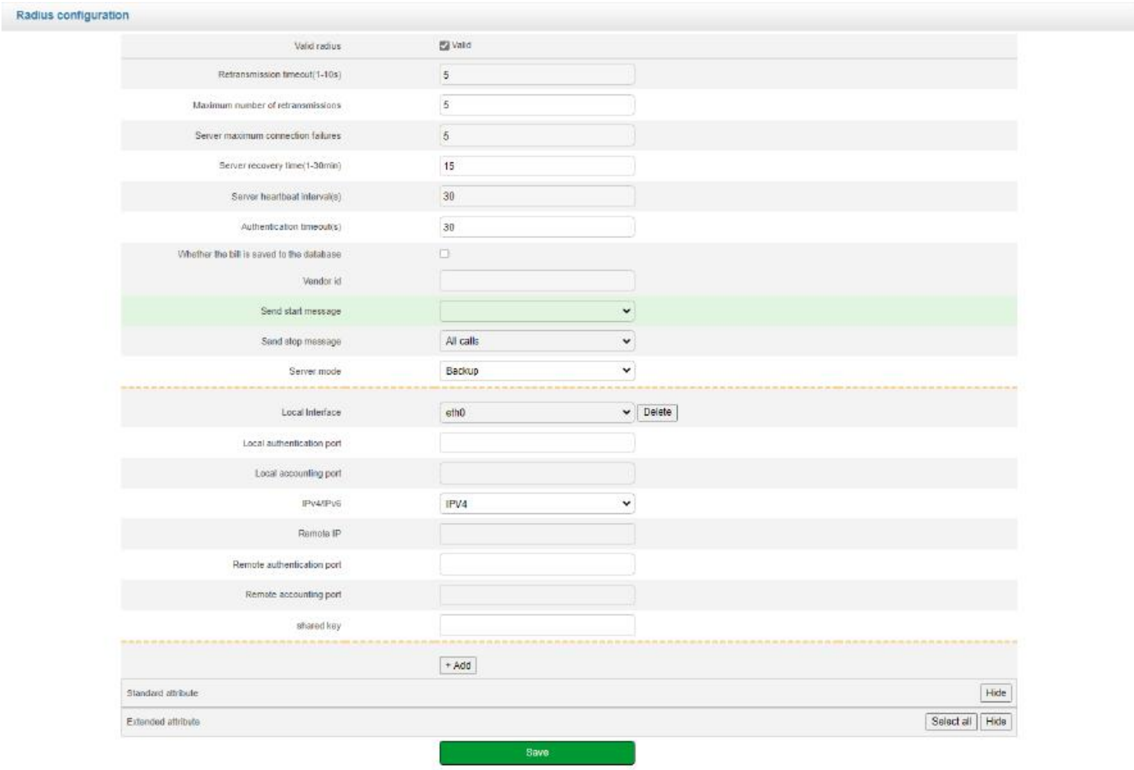


Figure 3-5-6 Radius configuration

Table 3-5-4 Radius configuration

Retransmission timeout(1-10s)	The re-transmission timeout of Radius messages
Maximum number of retransmissions	The maximum number of retransmissions of Radius messages
Server maximum connection failures	The server status is changed to failed after the Server maximum connection failures is exceeded
Server recovery time(1-30min)	Failed servers are automatically returned to a normal status after the Server recovery time
Server heartbeat interval(s)	Time interval of heartbeat messages for the interaction between the SBC and the server
Authentication timeout(s)	If the authentication response message is not received from the server after the Authentication

	timeout, the authentication is failed
Whether the bill is saved to the database	After you select this option, the system will save the CDRs to the database of SBC in advance. Then you can take out the CDRs from the database and send them to the server at once. You need to configure the number of CDRs to be taken from the database
Vendor id	Configure the Vendor ID of the radius server
Send start message	SBC sends accounting start message: Invite Message / Ringing / Connect
Send stop message	SBC sends accounting stop message: All calls / Normal call
Server mode	The policy of sending messages when there are multiple radius servers: Backup/Load Balance
Local Interface	The physical port where the radius messages of the SBC are sent
Local authentication port	The radius authentication listening port of SBC
Local accounting port	The radius accounting listening port of the SBC
IPv4/IPv6	The protocol type to interact with the server: IPv4/IPv6
Remote IP	The IP address of the Radius server
Remote authentication port	The authentication port of the Radius server

Remote accounting port	The accounting port of the Radius server
shared key	The shared key to interact with the Radius server
Standard/Extended attribute	The standard/extended attributes of Radius accounting messages

3.6 System

On the System pages, you can configure the device name, certification, network, port mapping, static routes, username & password as well as time zone & current time. You can also upgrade software versions, backup or restore configuration data, and update license and certificate.

3.6.1 System Management

On the **System->System Management** page, you can configure the name of the SBC8000.

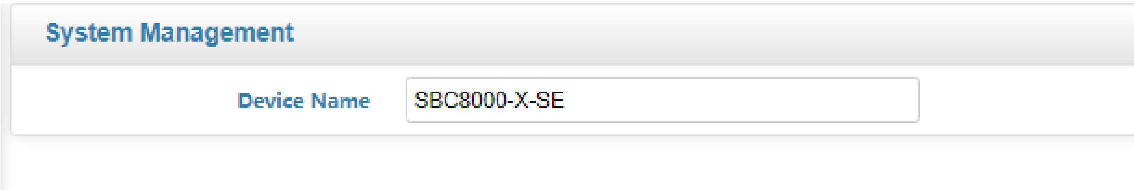


Figure 3-6-1 Device Name

3.6.2 Web Configuration

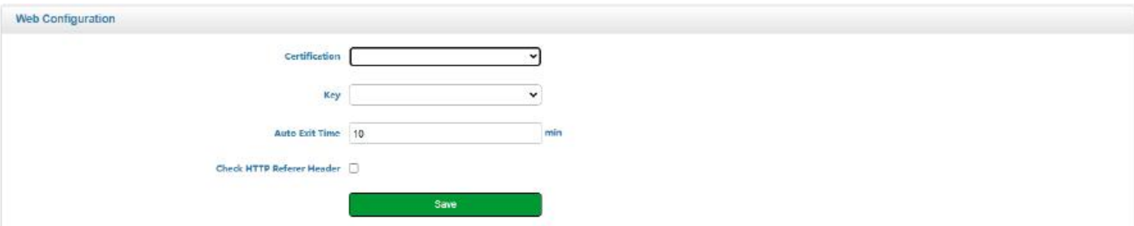


Figure 3-6-2 Web Configuration

Table 3-6-1 Web Configuration

Certification	You can select the CRT certificate used for https access
Key	You can select the Key certificate used for https access
Auto Exit Time	You can configure the Web auto-logout time
Check HTTP Referer Header	When it is enabled, the system will strictly check the HTTP Referer Header

3.6.3 Network

On the **System -> Network** page, you can configure the IP address, Subnet mask, gateway and DNS server. You can also add VLAN on the page.

Figure 3-6-3 Network Port

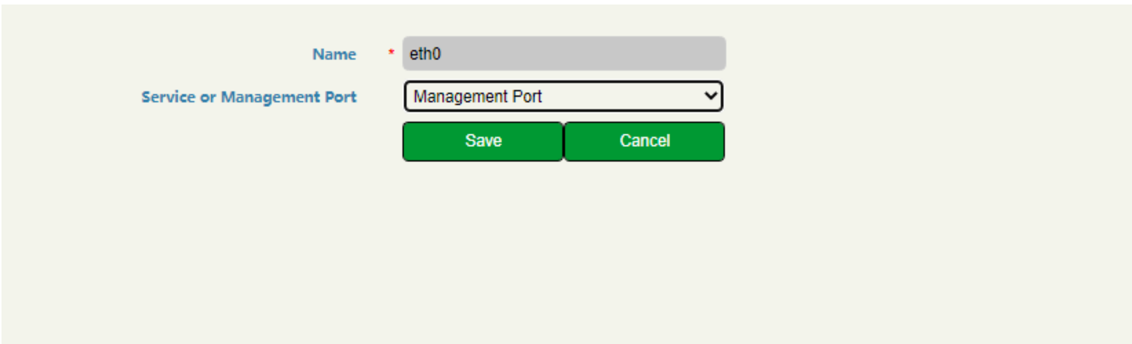


Figure 3-6-4 Modify Port Information

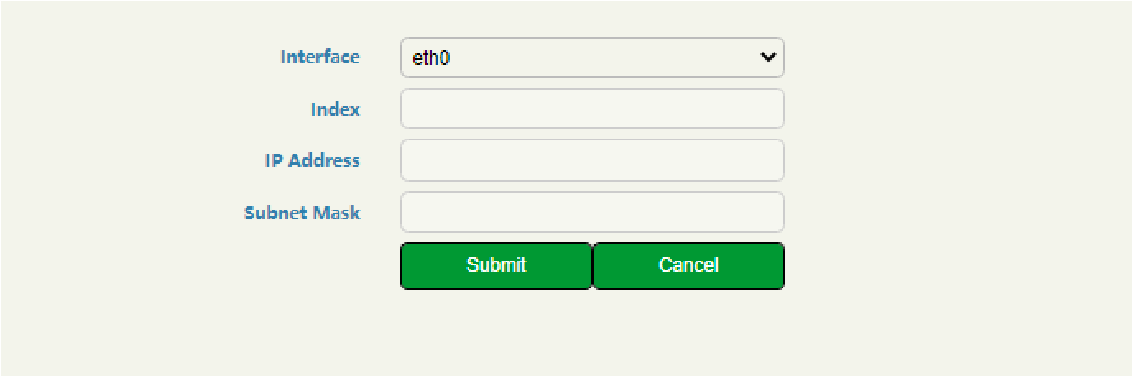


Figure 3-6-5 Add Floating IP

3.6.4 Static Route

On the **System->Static Route** page, you can configure static routes for the network. After a static route is successfully set, related packets will be sent to the designated destination according to the static route.

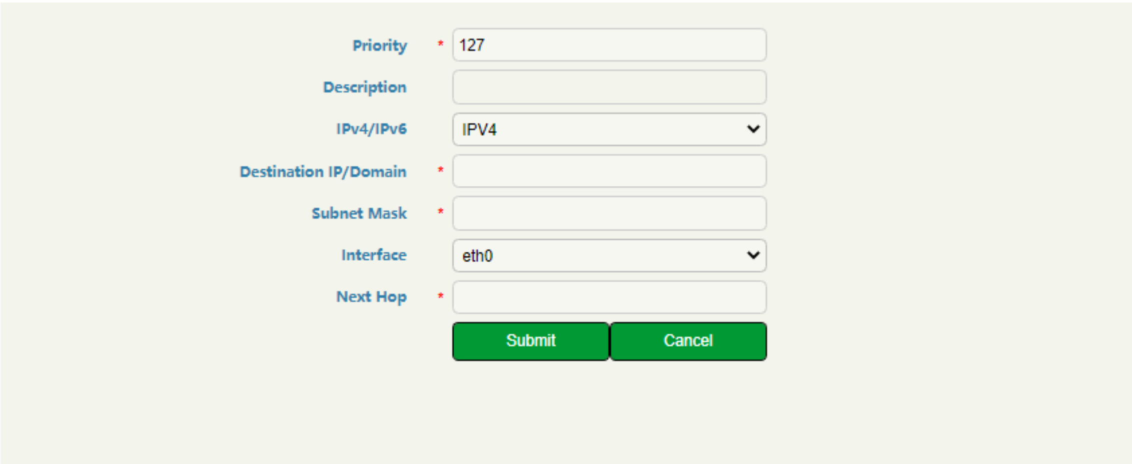


Figure 3-6-6 Add Static Route

Table 3-6-2 Static Route

Priority	The priority of the static route. The smaller digit, the higher priority
Description	The description of the static route
IPv4/IPv6	You can configure the protocol type: IPv4/IPv6

IP Destination/Domain	The destination IP address or domain of the static route
Subnet Mask	The netmask of the static route, such as 255.255.255.0
Interface	The source interface of the static route
Next Hop	The next hop address, namely the router address passed by the packets before they reach the destination address

3.6.5 User

On the **System->User->Password** page, you can modify administrator's password for logging in the SBC8000. Factory defaults for administrator's username and password are 'admin' and 'admin@123#' which are also used to log in SSH.

3.6.5.1 Password

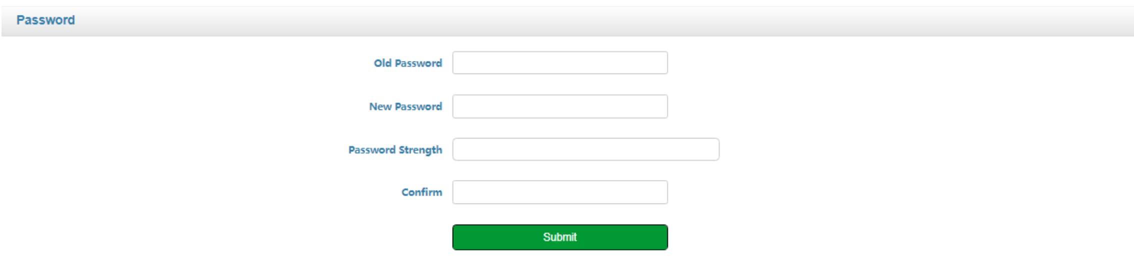


Figure 3-6-7 Modify Password

3.6.5.2 User List

On the **System->User->User List** page, the administrator can add the users that are allowed to log in the Web interface, specify their roles and set permissions to them.

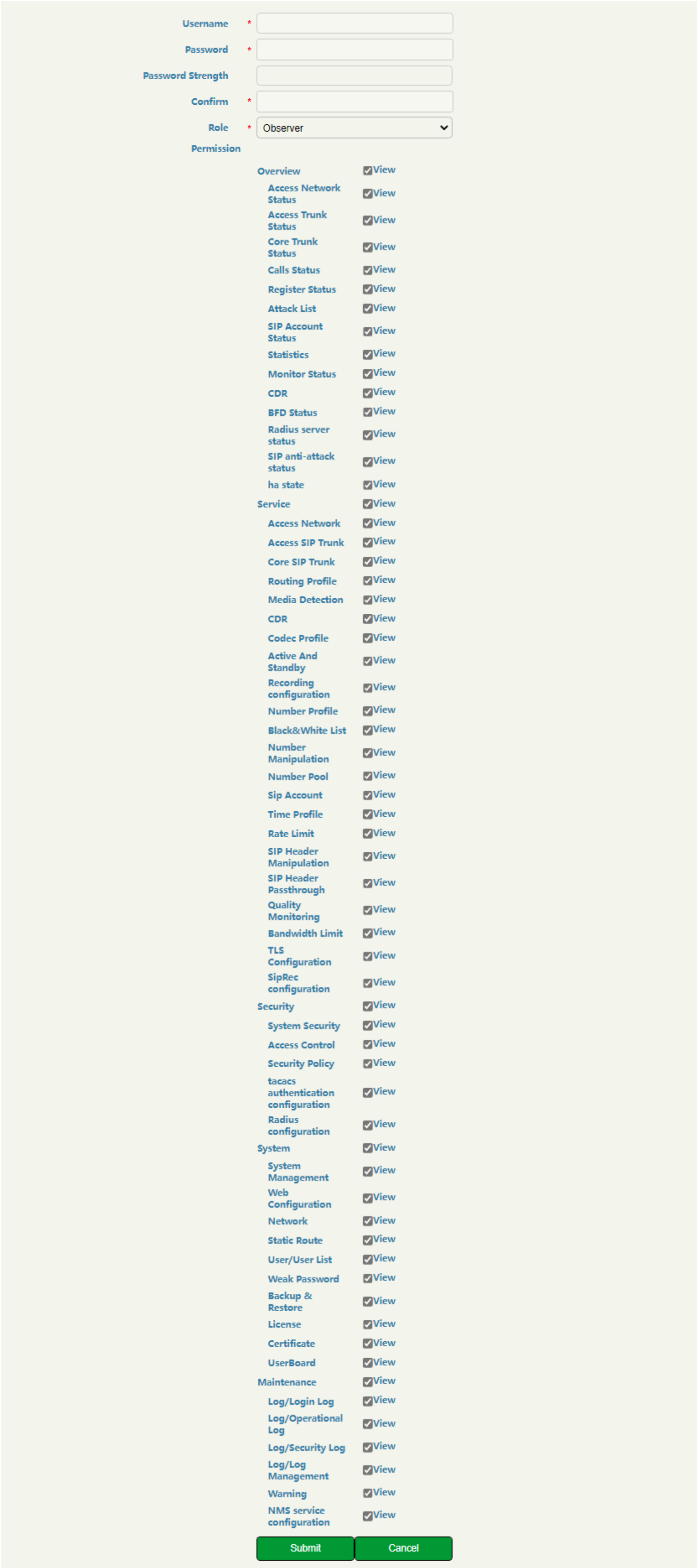


Figure 3-6-8 Add User and Assign Permissions

Table 3-6-3 User List

Username	The name of the user, which is used to log in the SBC8000
Password	The password for the user to log in the SBC8000 device
Password Strength	The security strength of the password
Confirm	Confirm the password
Role	Admin: has the permission to add users whose role is operator or observer, to modify the passwords of users, to add/delete/modify configurations. Only one administrator is allowed for one SBC8000. Operator: has the permission to view configurations, or modify part of the configurations. Observer: has the permission to view existing configurations, but cannot delete or modify them.

3.6.5.3 Weak Password

On this page, you can configure weak password for the system. The system will have a weak password prompt when setting the weak password.

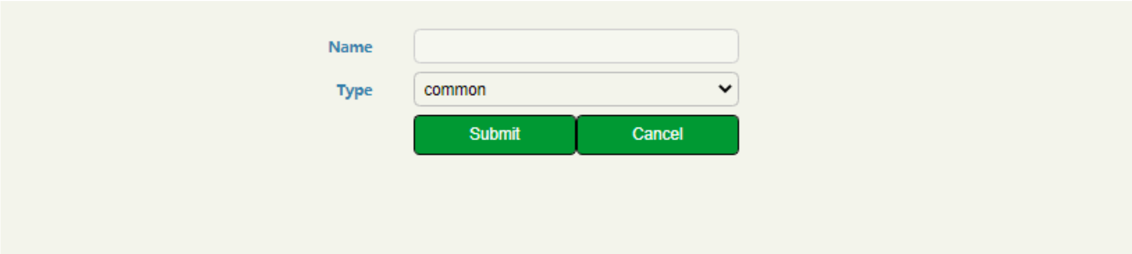


Figure 3-6-9 Weak Password

Table 3-6-4 Weak Password

Name	The name of weak paaword
Type	The type of weak password: common/bussiness

3.6.6 Backup & Restore

On the **System->Backup & Restore** interface, you can back up or restore all the configuration data, including service configurations, network configurations and license & certificate. After the configuration data is restored, the SBC8000 device will automatically restart.

Figure 3-6-10 Backup & Restore

Table 3-6-5 Backup & Restore

Backup	You can download the configuration data to be taken as backup. Select any of the checkboxes on the right of Service Config, Certification File and Network Config, and then click **Backup**
Restore	Choose a backup file, and then click **Restore**.

3.6.7 License

On the **System->License** page, the license information, including License Begin Time, License Total Time, License Expires,Max Media Sessions, Max Transcoding Sessions, Max Registered Users, RPS (registrations per second) and CPS(calls per second), is displayed. The SBC8000 device will not accept registrations and calls after the license expires.

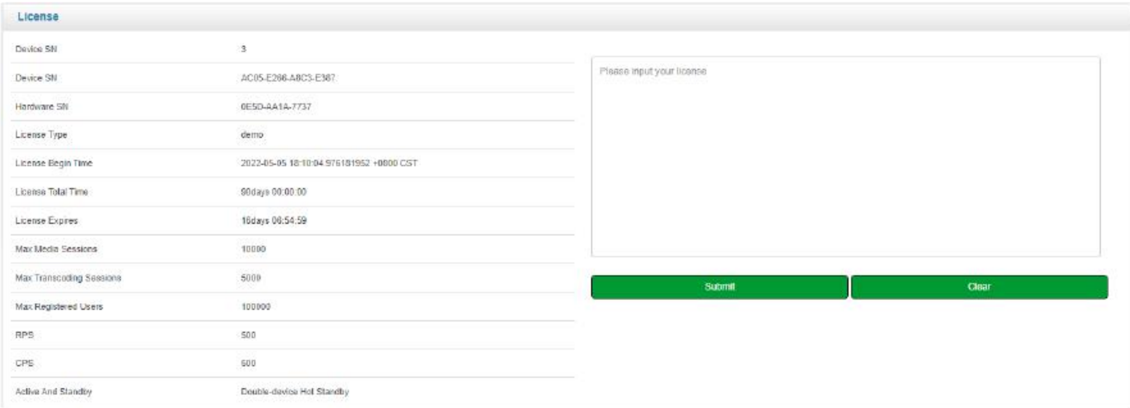


Figure 3-6-11 License Information

3.6.8 Certificate

On the **System->Certificate** page, you need to upload a certificate to ensure the secure login to the Web interface of the SBC8000. You can't log in the device until you has uploaded a certificate.

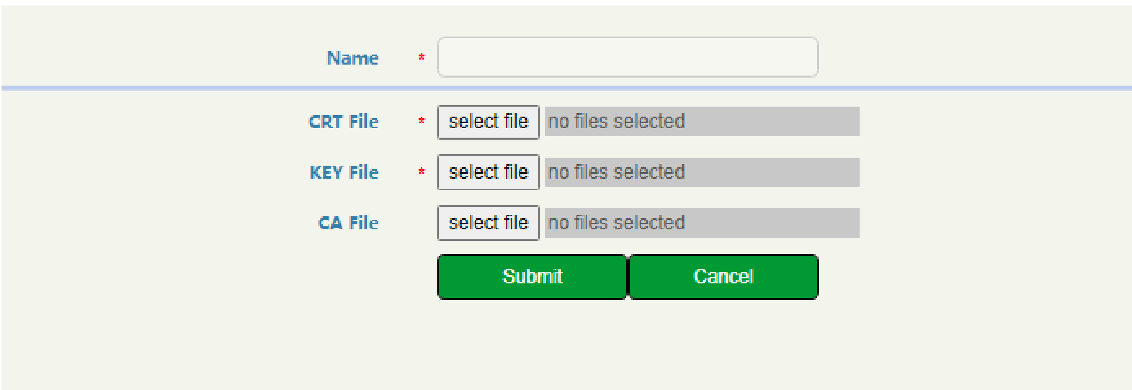


Figure 3-6-12 Upload Certificate

3.6.9 UserBoard

On this page, you can manage the number of user boards and the port range

Figure 3-6-13 UserBoard Management

3.7 Maintenance

3.7.1 Log

3.7.1.1 Login Log

The logs tracing the logins of the SBC8000 can be viewed on the **Maintenance->Login Log** page. You are allowed to set query criteria to view the logs that you want.

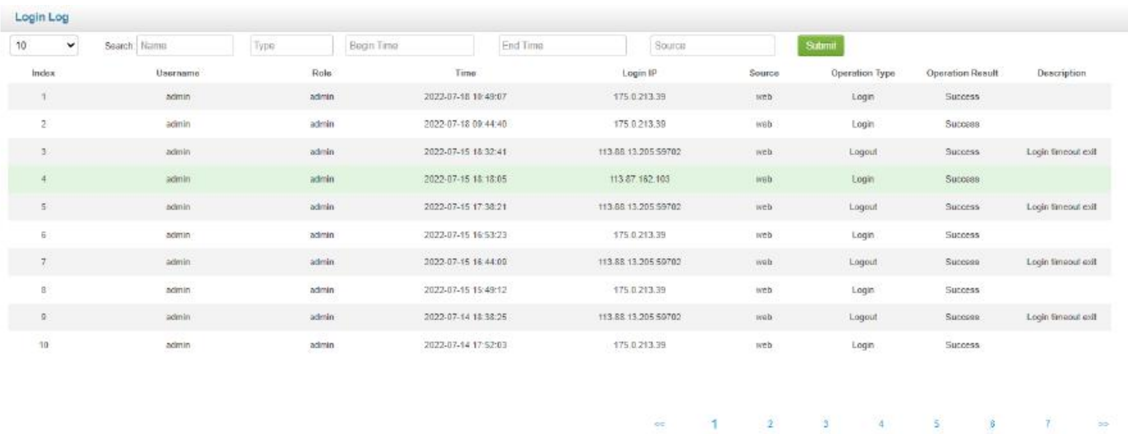
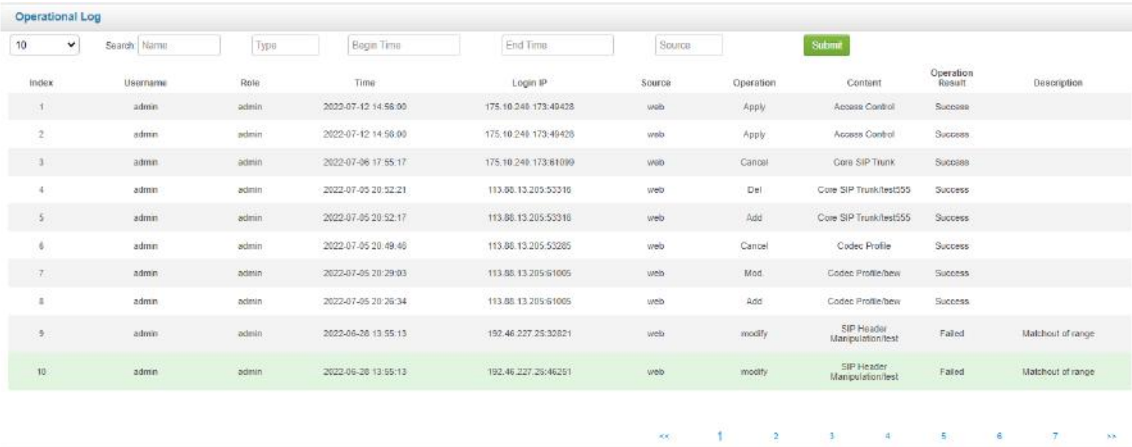


Figure 3-7-1 Login Log

3.7.1.2 Operational Log

The logs tracing the operations carried out on the Web interface can be queried on the **Maintenance -> Operation Log** page. You are allowed to set query criteria to view the logs that you want.


Operational Log

10 Search: Name Type Begin Time End Time Source Submit

Index	Username	Role	Time	Login IP	Source	Operation	Content	Operation Result	Description
1	admin	admin	2022-07-12 14:56:00	175.10.240.173:49428	web	Apply	Access Control	Success	
2	admin	admin	2022-07-12 14:56:00	175.10.240.173:49428	web	Apply	Access Control	Success	
3	admin	admin	2022-07-06 17:55:17	175.10.240.173:61099	web	Cancel	Core SIP Trunk	Success	
4	admin	admin	2022-07-05 20:52:21	113.88.13.205:53316	web	Del	Core SIP Trunk/test555	Success	
5	admin	admin	2022-07-05 20:52:17	113.88.13.205:53316	web	Add	Core SIP Trunk/test555	Success	
6	admin	admin	2022-07-05 20:49:46	113.88.13.205:53285	web	Cancel	Codec Profile	Success	
7	admin	admin	2022-07-05 20:29:03	113.88.13.205:61005	web	Mod.	Codec Profile/bew	Success	
8	admin	admin	2022-07-05 20:26:34	113.88.13.205:61005	web	Add	Codec Profile/bew	Success	
9	admin	admin	2022-06-28 13:55:13	192.46.227.25:32821	web	modify	SIP Header Manipulation/test	Failed	Matchout of range
10	admin	admin	2022-06-28 13:55:13	192.46.227.25:46251	web	modify	SIP Header Manipulation/test	Failed	Matchout of range

<< 1 2 3 4 5 6 7 >>

Figure 3-7-2 Operation Log

3.7.1.3 Security Log

The logs related to security can be viewed on the **Maintenance->Security Log** page. You are allowed to set query criteria to view the logs that you want.


Security Log

10 Search: Begin Time End Time Type Source IP Address Interface Port Submit

Index	Time	Attacked	Source	IP Address	Interface	Port	Condition	Action
1	2022-06-29 20:33:56	USER	SIP	40.77.85.230		58258	{"index":127,"describe":"Test Rule User Attack","condition":{"attackclass":"user","detectclass":"reg","value":4,"srctype":"AN","anname":""},"action":{"class":"block","value":0,"time":5}}	block

Figure 3-7-3 Security Log

3.7.1.4 Log Management

On the **Maintenance->Log Management** page, you can set the log level to filter logs, and can export the logs of different level.

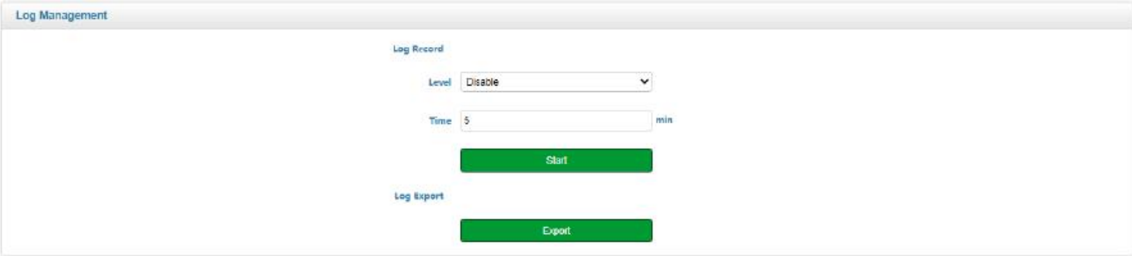


Figure 3-7-4 Log Management

3.7.1.5 Log Server

On the **Maintenance->Log Server** page, you can configure the parameters of Log Server.

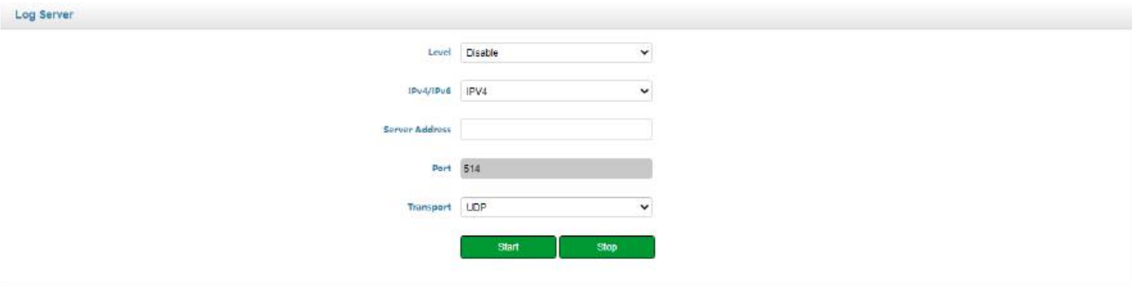


Figure 3-7-5 Log Server

Table 3-7-1 Log Server

Level	The levels of log: disable/emerg/alert/crit/err/warning/notice/info/debug
IPv4/IPv6	You can configure the protocol type: IPv4/IPv6
Server Address	The IP Address of Log Server
Port	The listening port of the log server, the default is 514 and it cannot be modified
Transport	The Transport protocols, you can select UDP/TCP

3.7.2 Reset

You can reset the Machine.

Figure 3-7-6 Reset

3.7.3 PING

Ping is used to examine whether a network works normally through sending test packets and calculating response time.

Instructions for using Ping:

1. Enter the IP address or domain name of a network, a website or a device in the input box of Ping, and then click **Start**.

2. If related messages are received, it means the network works normally; otherwise, the network is not connected or is connected faultily.

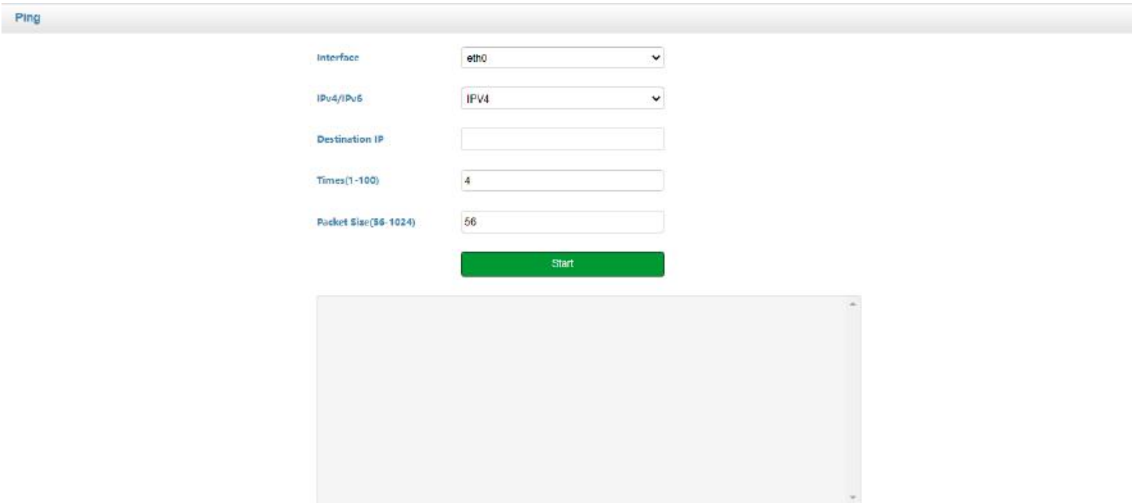


Figure 3-7-7 Ping

Table 3-7-2 Ping

Interface	Select the network interface for ping testing
IPv4/IPv6	Select network type, ipv4/ipv6
Destination IP	Ping test destination IP or domain name
Times(1-100)	Number of ping packets sent
Packet Size(56-1024)	Length of ping packets sent

3.7.4 Tracert

Tracert is used to determine a route from one IP address to another.

Instruction for using Traceroute:

1. Enter the IP address or domain name of a destination device in the input box of Tracert, and then click **Start**.
2. View the route information from the returned message.

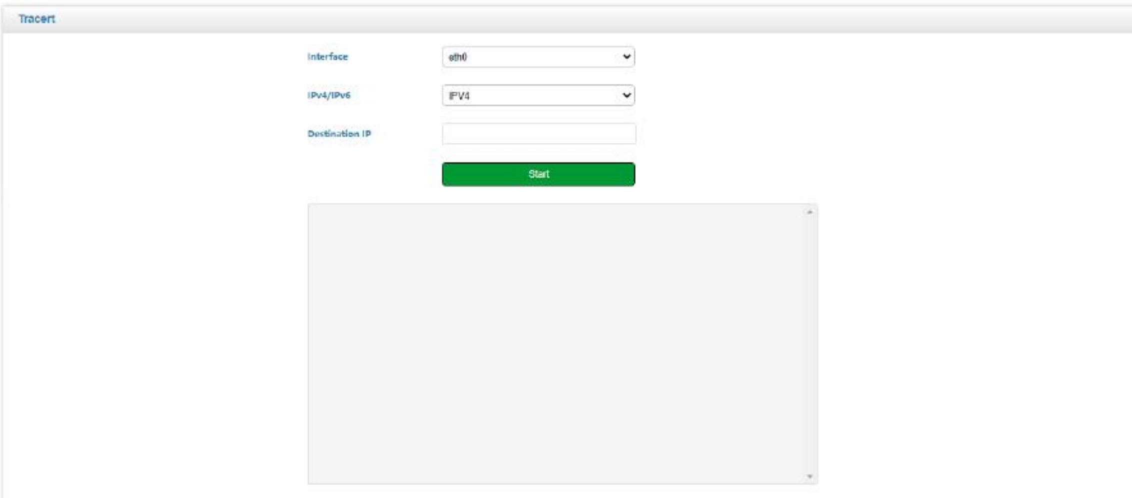


Figure 3-7-8 Tracert

Table 3-7-2 Tracert

Interface	Select the network interface for Tracert testing
IPv4/IPv6	Select network type, ipv4/ipv6
Destination IP	Tracert test destination IP or domain name

3.7.5 Regular Expression

On this page, the regular expression test verifies that the user's regular expression is correct and can be matched correctly.

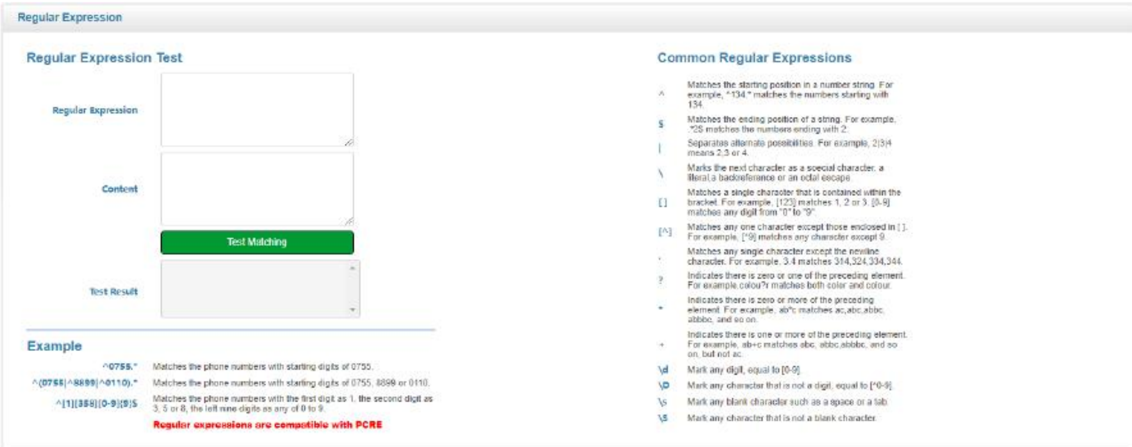


Figure 3-7-8 Regular Expression

3.7.6 Warning

The warning of the system can be displayed and can be filtered by conditions. The Warnings disappear after they are all confirmed.

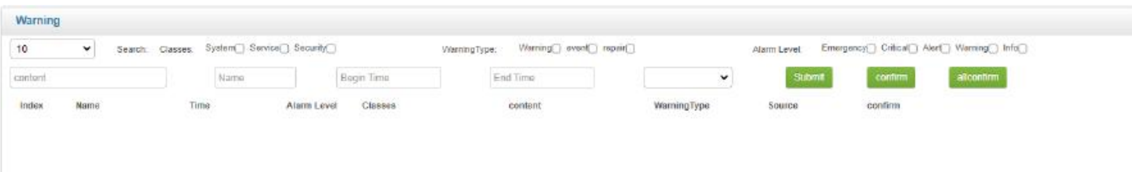


Figure 3-7-9 Warning

3.7.7 NMS Service Configuration

On this page, you can configure these parameters to connect with the NMS server for remote device management.

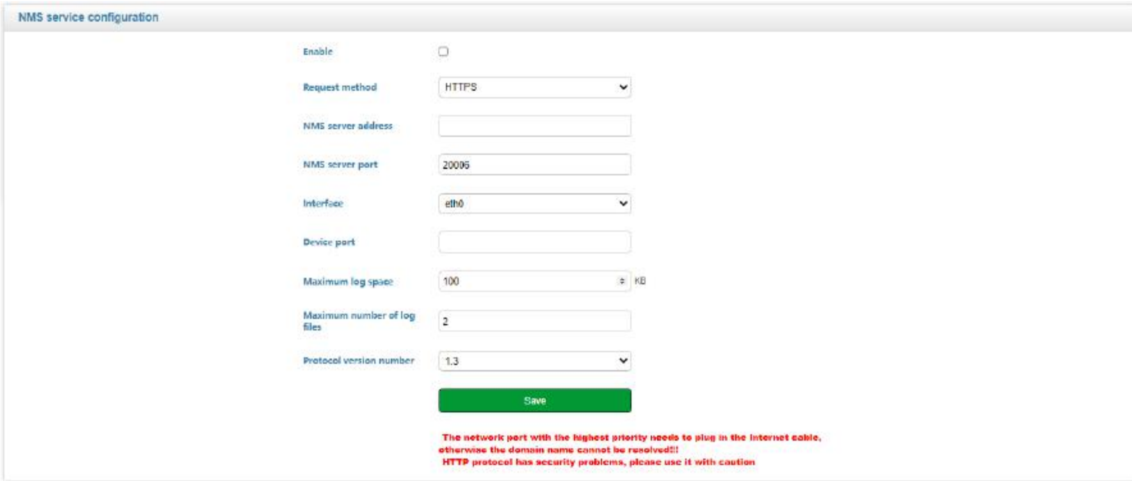


Figure 3-7-10 NMS service configuration

Table 3-7-3 NMS service configuration

Request method	The protocol used by SBC and NMS servers to interact, http/https. http protocol has security issues, please use with caution.
NMS server address	NMS server IP or domain name
NMS server port	NMS server listening port
Interface	Web interface to interact with the NMS server
Device port	SBC's nms service listening port
Maximum log space	Maximum file size for SBC and NMS interaction logs
Maximum number of log files	Max. number of SBC and NMS interaction logs

Protocol version number	Protocol version number of https

Notes:

1. The network port with the highest priority needs to plug in the Internet cable, otherwise the domain name cannot be resolved!

2. HTTP protocol has security problems, please use it with caution

4 Abbreviation

SBC: Session Border Controller

SIP: Session Initiation Protocol

DTMF: Dual Tone Multi Frequency

NAT: Network Address Translation

VLAN: Virtual Local Area Network

CID: Caller Identity

STUN: Simple Traversal of UDP over NAT

WLAN: Wireless Local Area Network