Configuration Note

AudioCodes Professional Services – Interoperability Lab

Amazon Chime Voice Connector SIPREC using AudioCodes Mediant™ SBC

Version 7.2

Table of Contents

This page is intentionally left blank.

Notice

Date Published: January-6-2020

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

Stay in the Loop with AudioCodes

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Document Revision Record

LTRT	Description
29325	Initial document release for Version 7.2.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at http://online.audiocodes.com/doc-feedback.

This page is intentionally left blank.

1 Introduction

This Configuration Note describes how to set up the AudioCodes Enterprise Session Border Controller (hereafter, referred to as *SBC*) for interworking with AWS Chime’s Voice Connector SIPREC environment.

1.1 Intended Audience

This document is intended for engineers, or AudioCodes and Generic partners who are responsible for installing and configuring Generic SIP Trunk and AWS Chime’s Voice Connector for enabling SIPREC streaming via AudioCodes SBC.

1.2 About AudioCodes SBC Product Series

AudioCodes' family of SBC devices enables reliable connectivity and security between the Enterprise's and the service provider's VoIP networks.

The SBC provides perimeter defense as a way of protecting Enterprises from malicious VoIP attacks; mediation for allowing the connection of any PBX and/or IP-PBX to any service provider; and Service Assurance for service quality and manageability.

Designed as a cost-effective appliance, the SBC is based on field-proven VoIP and network services with a native host processor, allowing the creation of purpose-built multiservice appliances, providing smooth connectivity to cloud services, with integrated quality of service, SLA monitoring, security and manageability. The native implementation of SBC provides a host of additional capabilities that are not possible with standalone SBC appliances such as VoIP mediation, PSTN access survivability, and third-party value-added services applications. This enables Enterprises to utilize the advantages of converged networks and eliminate the need for standalone appliances.

AudioCodes SBC is available as an integrated solution running on top of its field-proven Mediant Media Gateway and Multi-Service Business Router platforms, or as a software-only solution for deployment with third-party hardware. The SBC can be offered as a Virtualized SBC, supporting the following platforms: Hyper-V, AWS, AZURE, AWP, KVM and VMWare.

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes SBC Version

Table 2-1: AudioCodes SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500 Gateway & E-SBC ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 800C Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC ▪ Mediant 4000B SBC ▪ Mediant 9000 SBC ▪ Mediant 9030 SBC ▪ Mediant 9080 SBC ▪ Mediant Software SBC (VE/SE/CE)
Software Version	7.20A.254.475 or later
Protocol	▪ SIP/UDP or SIP/TCP (to the Generic SIP Trunk and IP-PBX) ▪ SIP/UDP (to the AWS Chime Voice Connector SIPREC service)
Additional Notes	None

2.2 Generic SIP Trunking Version

Table 2-2: Generic Version

Vendor/Service Provider	Generic
SSW Model/Service	
Software Version	
Protocol	SIP
Additional Notes	None

2.3 AWS Chime Voice Connector Version

Table 2-3: AWS Chime Voice Connector Version

Vendor	AWS Chime
Model	
Software Version	
Protocol	SIP
Additional Notes	None

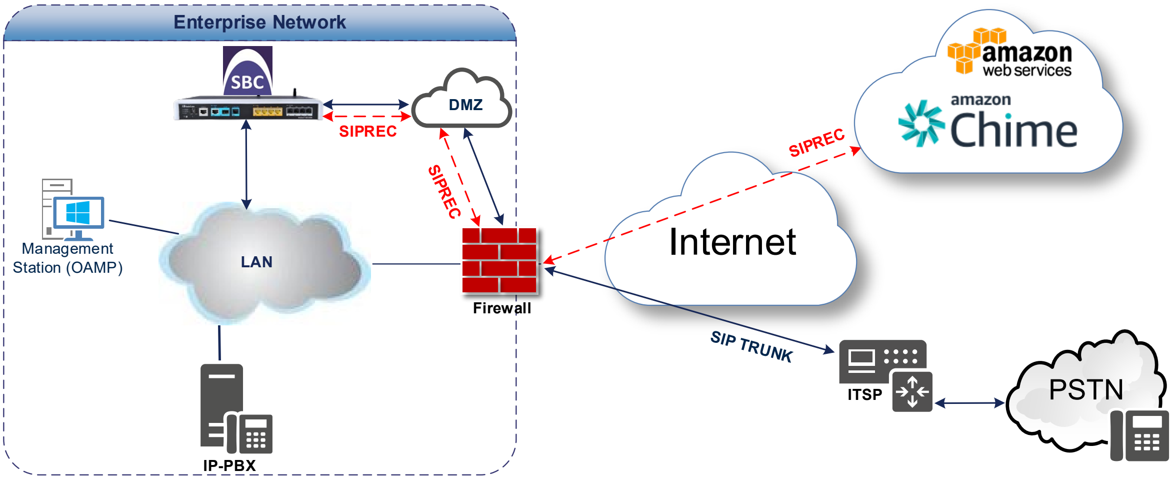
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes SBC and Generic SIP Trunk with the AWS Chime's Voice Connector system was done using the following topology setup:

- Enterprise deployed with IP-PBX and the administrator's management station, located on the LAN
- Enterprise deployed with the connection to AWS Chime's Voice Connector system located on the WAN
- Enterprise wishes to offer its employees enterprise-voice capabilities and to connect the Enterprise to the PSTN network using Generic's SIP Trunking service
- AudioCodes SBC is implemented to interconnect between the IP-PBX, SIP Trunk and the AWS Chime Voice Connector system
    - **Session:** Defines the Real-time voice session using the IP-based Session Initiation Protocol (SIP).
    - **Border:** Defines the IP-to-IP network border. The IP-PBX is located in the Enterprise LAN. The Generic's SIP Trunk and the AWS Chime's Voice Connector system are located in the public network.

The figure below illustrates this interoperability test topology:

Figure 2-1: Layout of an Interoperability Test Environment



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	▪ IP-PBX is located on the Enterprise's LAN ▪ Both, AWS Chime Voice Connector SIPREC system and Generic SIP Trunk environments are located on the WAN
Signaling Transcoding	▪ IP-PBX operates with SIP-over-UDP transport type ▪ AWS Chime Voice Connector SIPREC system operates with SIP-over-UDP or SIP-over-TCP or SIP-over-TLS transport types ▪ Generic SIP Trunk operates with SIP-over-TCP transport type
Codecs Transcoding	▪ IP-PBX supports G.711A-law, G.711U-law, and G.729 coders ▪ AWS Chime Voice Connector SIPREC system G.711U-law coder ▪ Generic SIP Trunk supports G.711A-law, G.711U-law, and G.729 coders
Media Transcoding	▪ IP-PBX operates with RTP media type ▪ AWS Chime Voice Connector SIPREC system operates with RTP or SRTP media types ▪ Generic SIP Trunk operates with RTP media type

2.4.2 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes SBC and the AWS Chime Voice Connector SIPREC system.

This page is intentionally left blank.

3 Configuring Amazon Chime Voice Connector

For configuring Amazon Chime Voice Connector, refer to
https://docs.aws.amazon.com/chime/latest/ag/voice-connectors.html.

This page is intentionally marked blank.

4 Configuring AudioCodes SBC

This section provides step-by-step procedures examples on how to configure AudioCodes SBC for enabling SIPREC streaming to the AWS Chime Voice Connector system for interworking between IP-PBX and the Generic SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

- **SBC LAN Interface:** Defines IP-PBX and Management Station
- **SBC WAN Interface:** Defines Generic SIP Trunking and the AWS Chime Voice Connector system environment

This configuration is done using the SBC's embedded Web server (hereafter, referred to as *Web interface*).

Notes:

- For implementing the SIPREC streaming to the AWS Chime Voice Connector system based on the configuration described in this section, AudioCodes SBC must be installed with a License Key that includes the following software features:
- **SIPREC Sessions** [Based on requirements]
- **Number of SBC sessions** [Based on requirements]
- **DSP Channels** [If media transcoding is needed]
- **Transcoding sessions** [If media transcoding is needed]

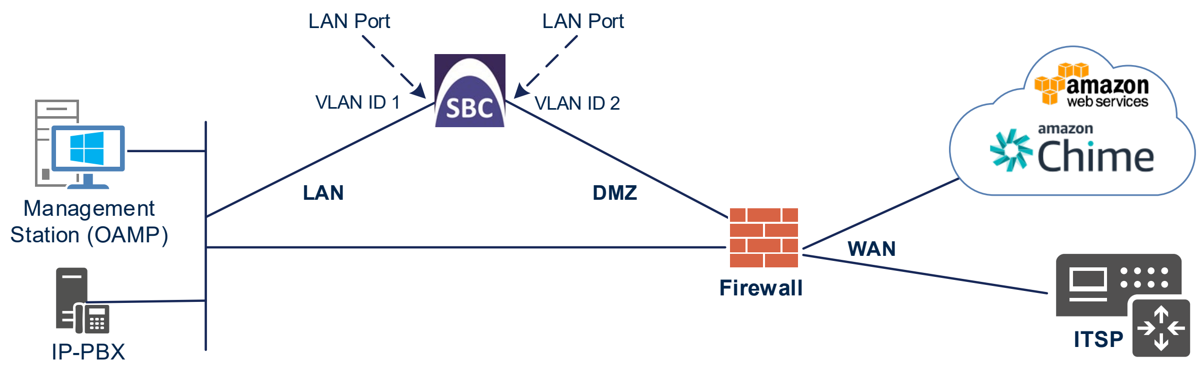
  For more information about the License Key, contact your AudioCodes sales representative.
- The scope of this document does **not** cover all security aspects for configuring this topology. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document, which can be found at AudioCodes web site

4.1 IP Network Interfaces Configuration

This section describes how to configure the SBC's IP network interfaces. There are several ways to deploy the SBC; however, this interoperability test topology employs the following deployment method:

- SBC interfaces with the following IP entities:
  - IP-PBX and Management Servers, located on the LAN
  - AWS Chime Voice Connector system and Generic SIP Trunk, located on the WAN
- SBC connects to the WAN through a DMZ network
- Physical connection: The type of physical connection depends on the method used to connect to the Enterprise's network. In the interoperability test topology, SBC connects to the LAN and DMZ using dedicated Ethernet ports (i.e., two ports and two network cables are used).
- SBC also uses two logical network interfaces:
  - LAN (VLAN ID 1)
  - DMZ (VLAN ID 2)

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 Configure VLANs

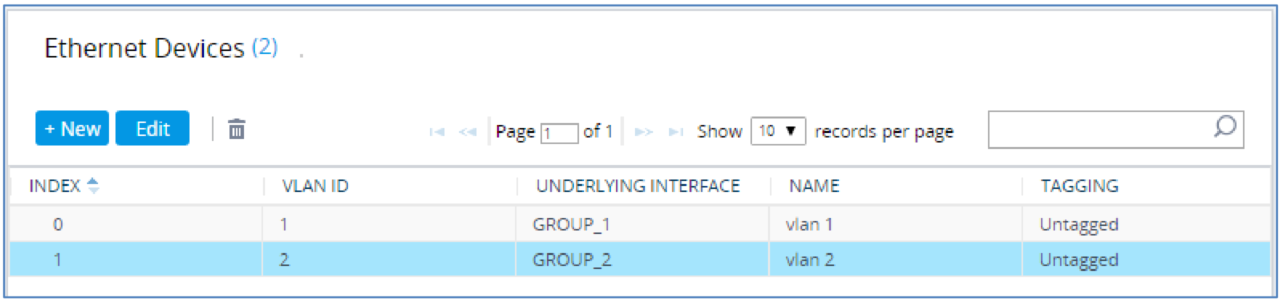
This section describes how to configure VLANs for each of the following interfaces:

- LAN VoIP (assigned the name "LAN_IF")
- WAN VoIP (assigned the name "WAN_IF")

➢ **To configure the VLANs:**

1. Open the Ethernet Device table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet Devices**).
2. There will be one existing row for VLAN ID 1 and underlying interface GROUP_1.
3. Add another VLAN ID 2 for the WAN side

Figure 4-2: Configured VLAN IDs in Ethernet Device



INDEX	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING
0	1	GROUP_1	vlan 1	Untagged
1	2	GROUP_2	vlan 2	Untagged

4.1.2 Configure Network Interfaces

This section describes how to configure the IP network interfaces for each of the following interfaces:

- LAN Interface (assigned the name "LAN_IF")
- WAN Interface (assigned the name "WAN_IF")

➢ **To configure the IP network interfaces:**

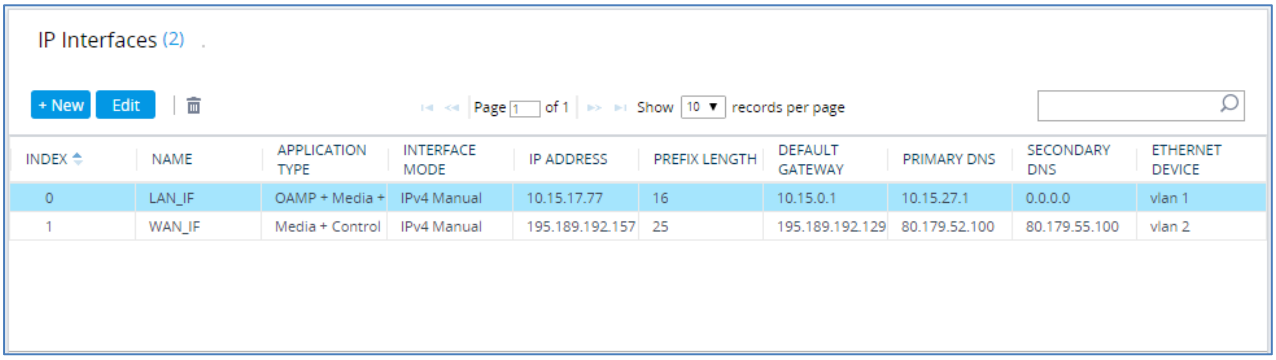
1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Configure the IP interfaces as follows (your network parameters might be different):

Table 4-1: Configuration Example of the Network Interface Table

Index	Application Types	Interface Mode	IP Address	Prefix Length	Gateway	DNS	I/F Name	Ethernet Device
0	OAMP+ Media + Control	IPv4 Manual	10.15.77.77	16	10.15.0.1	10.15.27.1	LAN_IF	vlan 1
1	Media + Control (as this interface points to the internet, enabling OAMP is not recommended)	IPv4 Manual	195.189.192.157 (DMZ IP address of SBC)	25	195.189.192.129 (router's IP address)	According to your Internet provider's instructions	WAN_IF	vlan 2

The configured IP network interfaces are shown below:

Figure 4-3: Configured Network Interfaces in IP Interfaces Table



4.2 Configure Media Realms

This section describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **To configure Media Realms:**

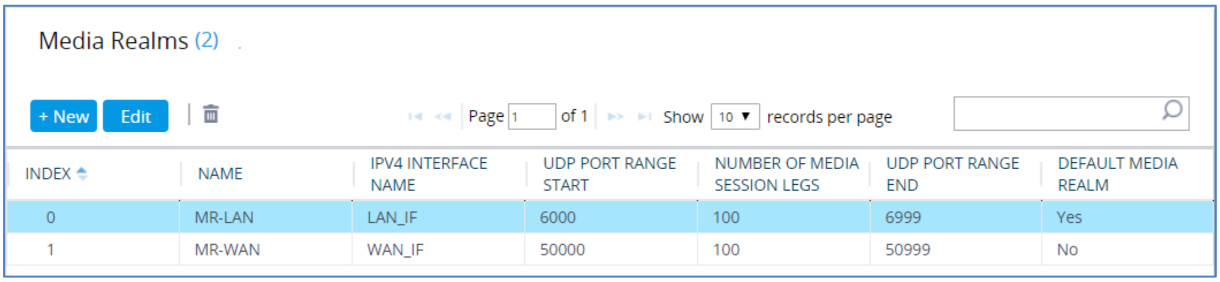
1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Configure Media Realm as follows (you can use the default Media Realm (Index 0), but modify it):

Table 4-2: Configuration Example Media Realms in Media Realm Table

Index	Name	IPv4 Interface Name	Port Range Start	Number of Media Session Legs
0	MR-LAN (arbitrary name)	LAN_IF	6000	100 (media sessions assigned with port range)
1	MR-WAN (arbitrary name)	WAN_IF	50000	100 (media sessions assigned with port range)
All other parameters can be left unchanged at their default values.				

The configured Media Realm is shown in the figure below:

Figure 4-4: Configured Media Realm in Media Realm Table



4.3 Configure SIP Signaling Interfaces

This section describes how to configure SIP Interfaces. For the interoperability test topology, an internal and external SIP Interface must be configured for the SBC.

➢ **To configure SIP Interfaces:**

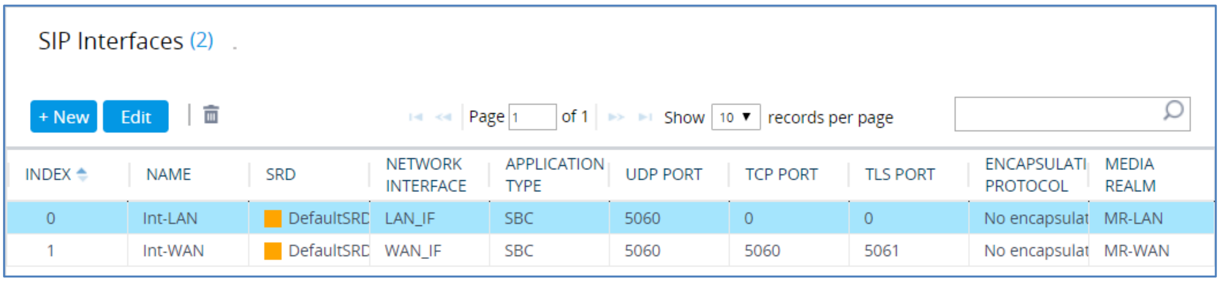
1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Configure SIP Interface. You can use the default SIP Interface (Index 0), but modify it as shown in the table below. The table below shows an example of the configuration. You can change some parameters according to your requirements.

Table 4-3: Configured SIP Interface in SIP Interface Table

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Media Realm
0	**Int-LAN** (arbitrary name)	**LAN_IF**	**SBC**	**5060** (according to requirement)	**0**	**0**	**MR-LAN**
0	**Int-WAN** (arbitrary name)	**WAN_IF**	**SBC**	**5060** (according to requirement)	**5060** (according to requirement)	**5061** (according to requirement)	**MR-WAN**
All other parameters can be left unchanged at their default values.							

The configured SIP Interface is shown in the figure below:

Figure 4-5: Configured SIP Interface in SIP Interface Table



4.4 Configure Proxy Sets and Proxy Address

This section describes how to configure Proxy Sets. The Proxy Set defines the destination address (IP address or FQDN) of the IP entity server. Proxy Sets can also be used to configure load balancing between multiple servers.

For the interoperability test topology, two Proxy Sets need to be configured for the following IP entities:

- IP-PBX
- Generic SIP Trunk
- AWS Chime Voice Connector system

The Proxy Sets will later be applied to the VoIP network by assigning them to IP Groups.

➢ **To configure Proxy Sets:**

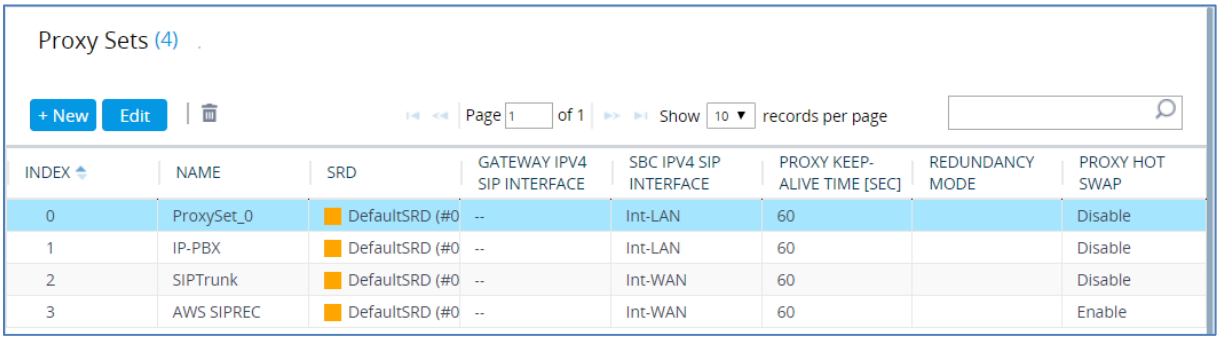
1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Configure Proxy Sets as shown in the table below:

Table 4-4: Configuration Example Proxy Sets in Proxy Sets Table

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive	Proxy Hot Swap
1	**IP-PBX** (arbitrary name)	Int-LAN	Default	Using Options	Disable
2	**SIPTrunk** (arbitrary name)	Int-WAN	Default	Using Options	Disable
3	**AWS SIPREC** (arbitrary name)	Int-WAN	Default	Using Options	Enable

The configured Proxy Sets are shown in the figure below:

Figure 4-6: Configured Proxy Sets in Proxy Sets Table



INDEX	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD (#0	--	Int-LAN	60		Disable
1	IP-PBX	DefaultSRD (#0	--	Int-LAN	60		Disable
2	SIPTrunk	DefaultSRD (#0	--	Int-WAN	60		Disable
3	AWS SIPREC	DefaultSRD (#0	--	Int-WAN	60		Enable

4.4.1 Configure a Proxy Address

This section shows how to configure a Proxy Address.

➢ **To configure a Proxy Address for IP-PBX:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) and then click the Proxy Set **IP-PBX**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**; the following dialog box appears:

Figure 4-7: Configuring Proxy Address for IP-PBX

3. Configure the address of the Proxy Set according to the parameters described in the table below:

Table 4-5: Configuration Proxy Address for IP-PBX

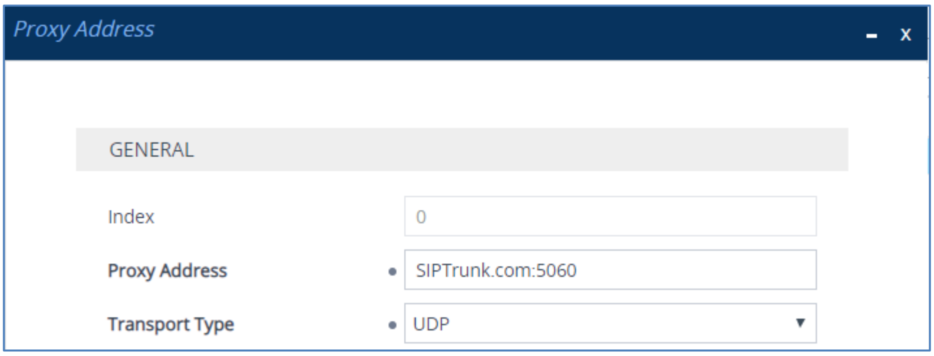
Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	**10.10.10.10:5060** (SIP Trunk IP / FQDN and port)	UDP	0	0

4. Click **Apply**.

➢ **To configure a Proxy Address for SIP Trunk:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) and then click the Proxy Set **SIPTrunk**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**; the following dialog box appears:

Figure 4-8: Configuring Proxy Address for SIP Trunk



3. Configure the address of the Proxy Set according to the parameters described in the table below:

Table 4-6: Configuration Proxy Address for SIP Trunk

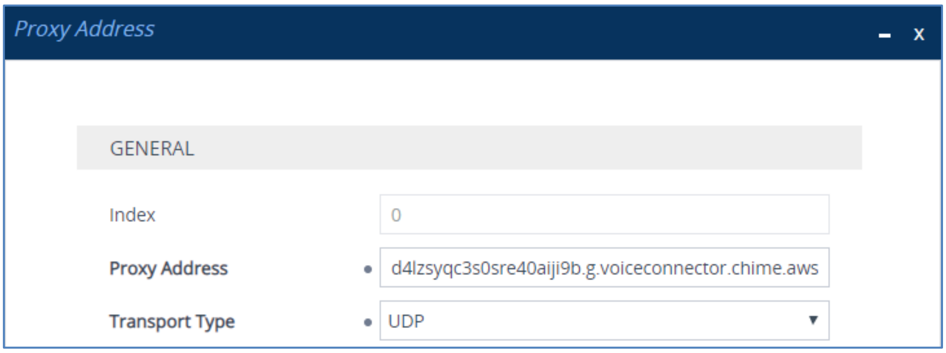
Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	**SIPTrunk.com:5060** (SIP Trunk IP / FQDN and port)	UDP	0	0

4. Click **Apply**.

➢ **To configure a Proxy Address for the AWS Chime Voice Connector:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) and then click the Proxy Set **AWS SIPREC**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**; the following dialog box appears:

Figure 4-9: Configuring Proxy Address for AWS Chime Voice Connector Interface



3. Configure the address of the Proxy Set according to the parameters described in the table below:

Table 4-7: Configuration Proxy Address for UDP connection to AWS Chime Voice Connector

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	**d4lzsyqc3s0sre40aiji9b.g.voiceconnector.chime.aws:5060**	UDP	0	0

4. Click **Apply**.

Note: The connection to the AWS Chime Voice Connector may change according to your specific deployment topology (UDP, TCP or TLS). Refer to AWS Chime Voice Connector support website for specific addresses.

4.5 Configure Coders

This section describes how to configure coders (termed *Coder Group*). As the IP-PBX and SIP Trunk may support different coders while the Generic Voice Connector supports only G.711 U-law coder, you need to add a Coder Group with the G.711 U-law coder for the Generic Voice Connector.

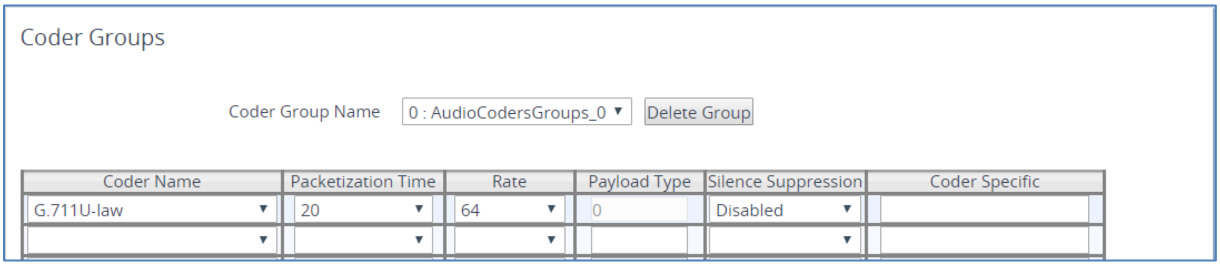
Note that the Coder Group ID for this entity will be assigned to its corresponding IP Profile in the next step.

➢ **To configure coders:**

1. Open the Coder Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Coder Groups**).
2. Configure a Coder Group for the AWS Chime Voice Connector:

Parameter	Value
Coder Group Name	**AudioCodersGroups_0**
Coder Name	**G.711 U-law**

Figure 4-10: Configuring Coder Group for AWS Chime Voice Connector



3. Click **Apply**.

4.6 Configure IP Profiles

This section describes how to configure IP Profiles. The IP Profile defines a set of call capabilities relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder and transcoding method).

In this interoperability test topology, IP Profiles need to be configured for the following IP entities:

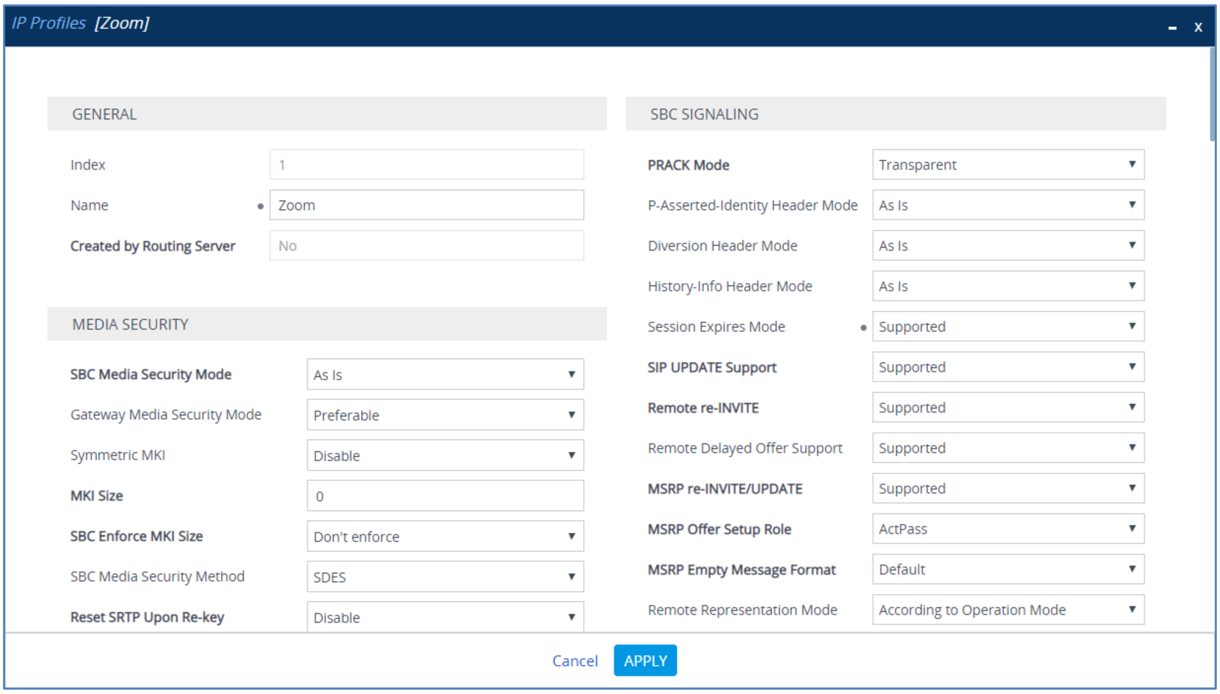
- IP-PBX – to operate in non-secure mode using RTP and SIP over UDP
- Generic SIP Trunk – to operate in non-secure mode using RTP and SIP over UDP
- AWS Chime Voice Connector SIPREC – to operate in non-secure mode using RTP and SIP over UDP

➤ **To configure IP Profile for the IP-PBX:**

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **New**, and then configure the parameters as follows:

Parameter	Value
General	
Index	**1**
Name	**IP-PBX** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**Not Secured**
SBC Media	
Extension Coders Group	**AudioCodersGroups_0**

Figure 4-11: Configuring IP Profile for IP-PBX



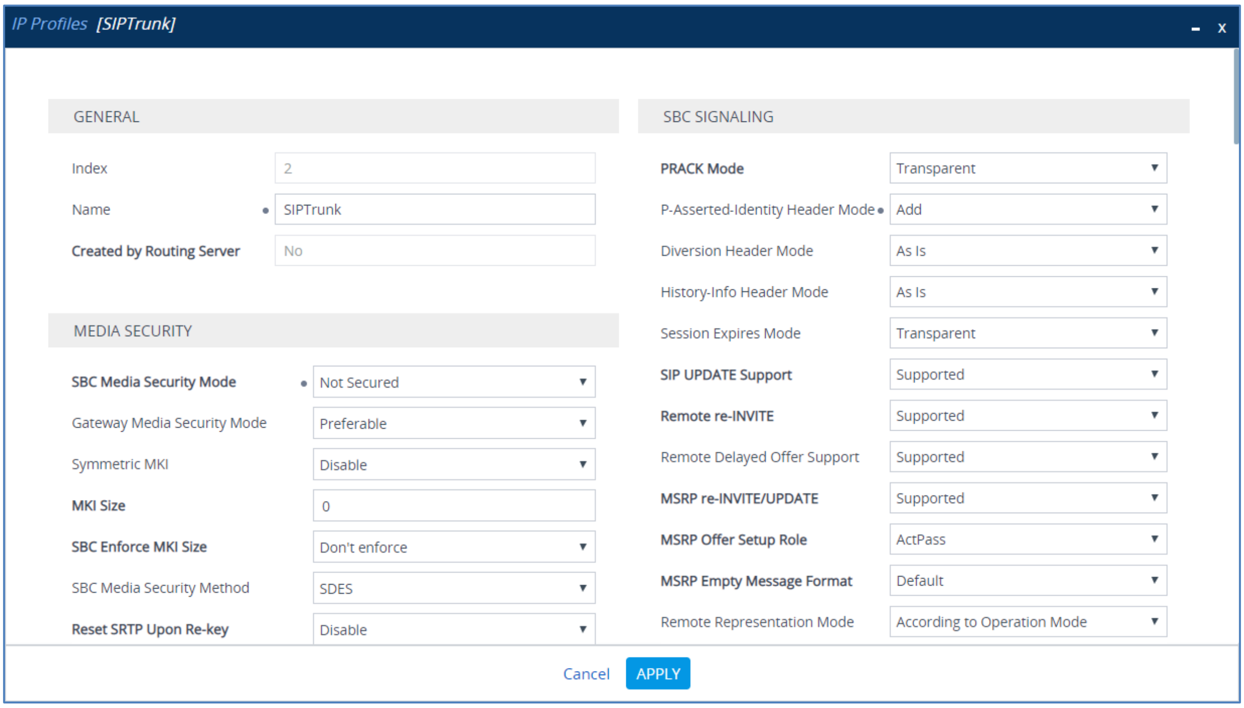
3. Click **Apply**.

➢ To configure an IP Profile for the Generic SIP Trunk:

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **New**, and then configure the parameters as follows:

Parameter	Value
General	
Index	**2**
Name	**SIPTrunk**
Media Security	
SBC Media Security Mode	**Not Secured**
SBC Media	
Extension Coders Group	**AudioCodersGroups_0**
SBC Signaling	
P-Asserted-Identity Header Mode	**Add** (required for anonymous calls)

Figure 4-12: Configuring IP Profile for Generic SIP Trunk



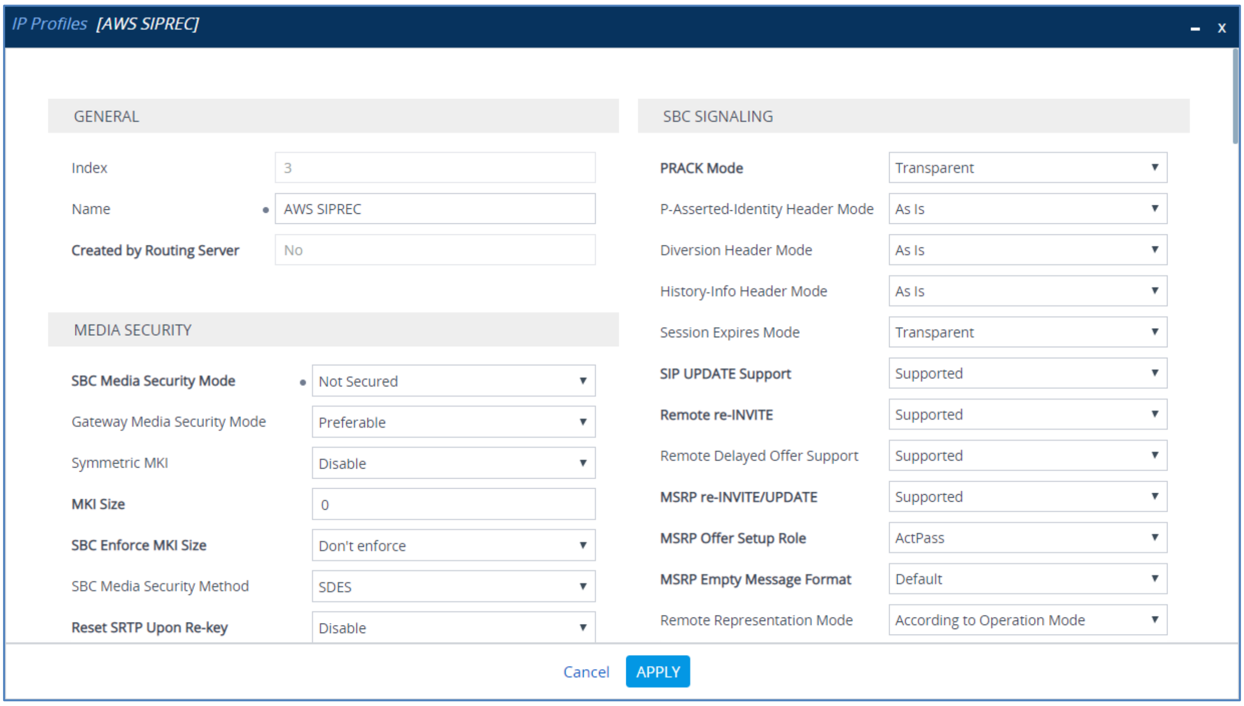
3. Click **Apply**.

➢ To configure IP Profile for the AWS Chime Voice Connector:

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **New**, and then configure the parameters as follows:

Parameter	Value
General	
Index	**3**
Name	**AWS SIPREC** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**Not Secured**
SBC Media	
Extension Coders Group	**AudioCodersGroups_0**

Figure 4-13: Configuring IP Profile for AWS Chime Voice Connector



3. Click **Apply**.

4.7 Configure IP Groups

This section describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the SBC communicates. This can be a server (e.g., IP-PBX or ITSP) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

In this interoperability test topology, IP Groups must be configured for the following IP entities:

- IP-PBX
- Generic SIP Trunk
- AWS Chime Voice Connector SIPREC service

➢ **To configure IP Groups:**

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Configure an IP Group for the IP-PBX:

Parameter	Value
Index	**1**
Name	**IP-PBX**
Type	**Server**
Proxy Set	**IP-PBX**
IP Profile	**IP-PBX**
Media Realm	**MR-Lan**
SIP Group Name	(according to requirement)

3. Configure an IP Group for the Generic SIP Trunk:

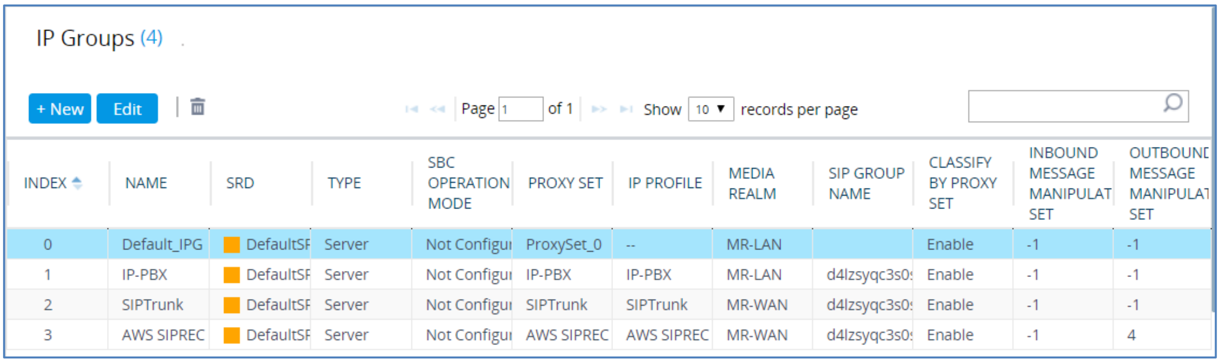
Parameter	Value
Index	**1**
Name	**SIPTrunk**
Type	**Server**
Proxy Set	**SIPTrunk**
IP Profile	**SIPTrunk**
Media Realm	**MR-Wan**
SIP Group Name	(according to requirement)

4. Configure an IP Group for the AWS Chime Voice Connector SIPREC service:

Parameter	Value
Index	**3**
Name	**AWS SIPREC**
Type	**Server**
Proxy Set	**AWS SIPREC**
IP Profile	**AWS SIPREC**
Media Realm	**MR-Wan**
SIP Group Name	(according to requirement)

The configured IP Groups are shown in the figure below:

Figure 4-14: Configured IP Groups in IP Group Table



IP Groups (4)

+ New | Edit | Page 1 of 1 | Show 10 records per page

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULAT SET	OUTBOUND MESSAGE MANIPULAT SET
0	Default_IPG	DefaultSF	Server	Not Configui	ProxySet_0	--	MR-LAN		Enable	-1	-1
1	IP-PBX	DefaultSF	Server	Not Configui	IP-PBX	IP-PBX	MR-LAN	d4lzsyqc3s0:	Enable	-1	-1
2	SIPTrunk	DefaultSF	Server	Not Configui	SIPTrunk	SIPTrunk	MR-WAN	d4lzsyqc3s0:	Enable	-1	-1
3	AWS SIPREC	DefaultSF	Server	Not Configui	AWS SIPREC	AWS SIPREC	MR-WAN	d4lzsyqc3s0:	Enable	-1	4

4.8 SIP TLS Connection Configuration (Optional)

This section describes how to configure the SBC for using a TLS connection. It can be required for connection with the Generic SIP Trunk or with AWS Chime Voice Connector. This is essential for a secure SIP TLS connection and highly recommended by Amazon.

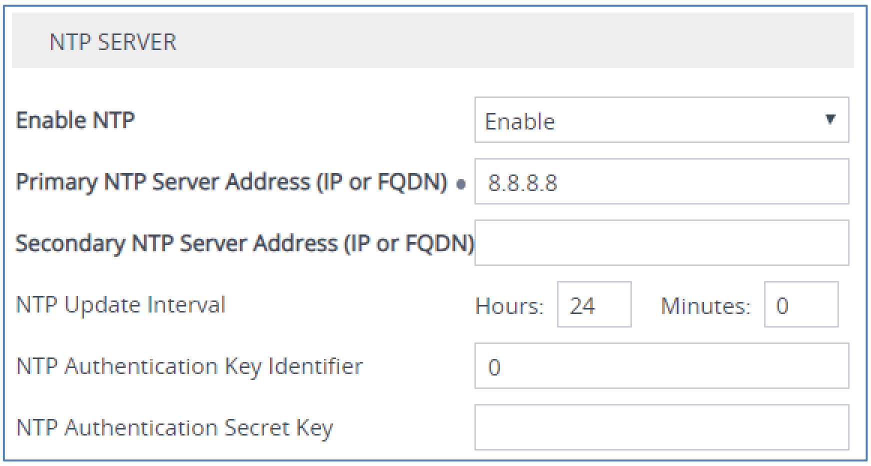
4.8.1 Configure the NTP Server Address

This step describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or a third-party server) to ensure that the SBC receives the accurate and current date and time. This is necessary for validating certificates of remote parties.

➢ **To configure the NTP server address:**

1. Open the Time & Date page (**Setup** menu > **Administration** tab > **Time & Date**).
2. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., **8.8.8.8**).

Figure 4-15: Configuring NTP Server Address



3. Click **Apply**.

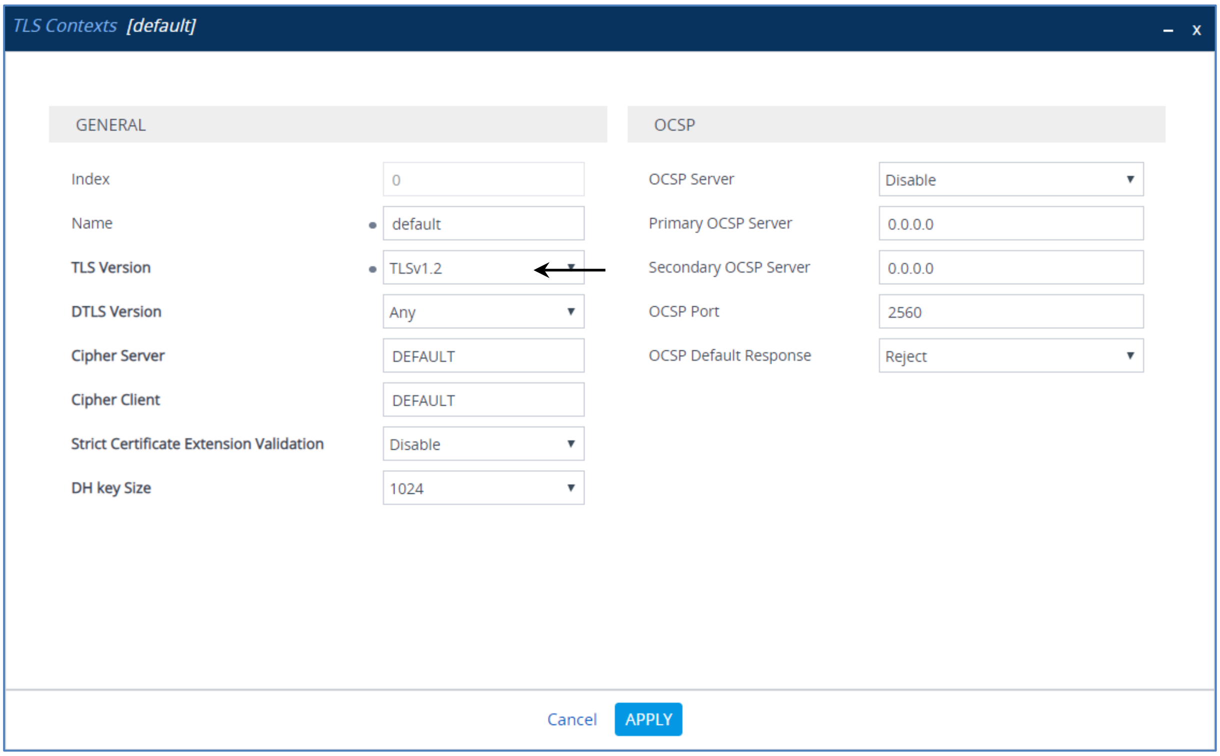
4.8.2 Configure the TLS version

This step describes how to configure the SBC to use TLS version 1.2 only. AudioCodes recommends implementing only TLS to avoid flaws in SSL.

➢ **To configure the TLS version:**

1. Open the TLS Contexts table (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts table, select the required TLS Context index row (usually default index 0 will be used), and then click '**Edit**'.
3. From the '**TLS Version**' drop-down list, select '**TLSv1.2**'

Figure 4-16: Configuring TLS version



4. Click **Apply**.

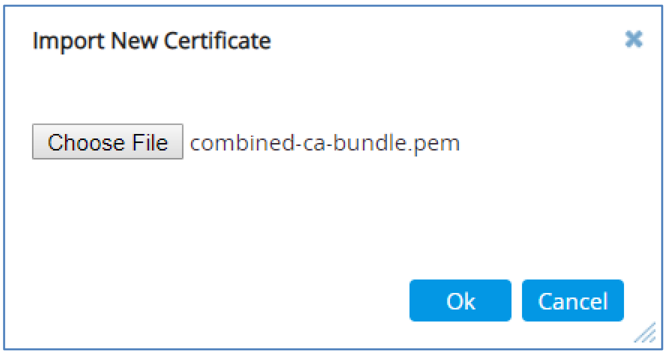
4.8.3 Deploy Amazon Trusted Root Certificate

This step describes how to import the Amazon Chime root certificate. Currently the Amazon Chime Voice Connector service uses a wildcard certificate (*.voiceconnector.chime.aws). To trust this certificate, your SBC *must* import this certificate to its Trusted Certificates storage. Download the certificate from https://s3.amazonaws.com/voice-connector-certs/combined-ca-bundle.pem. Follow the steps below to import the certificate to the Trusted Root storage.

➢ **To configure a certificate:**

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the required TLS Context index row, and then click the **Trusted Root Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
3. Click the **Import** button, and then select the certificate file to load:

Figure 4-17: Importing Root Certificate into Trusted Certificates Store



4. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.

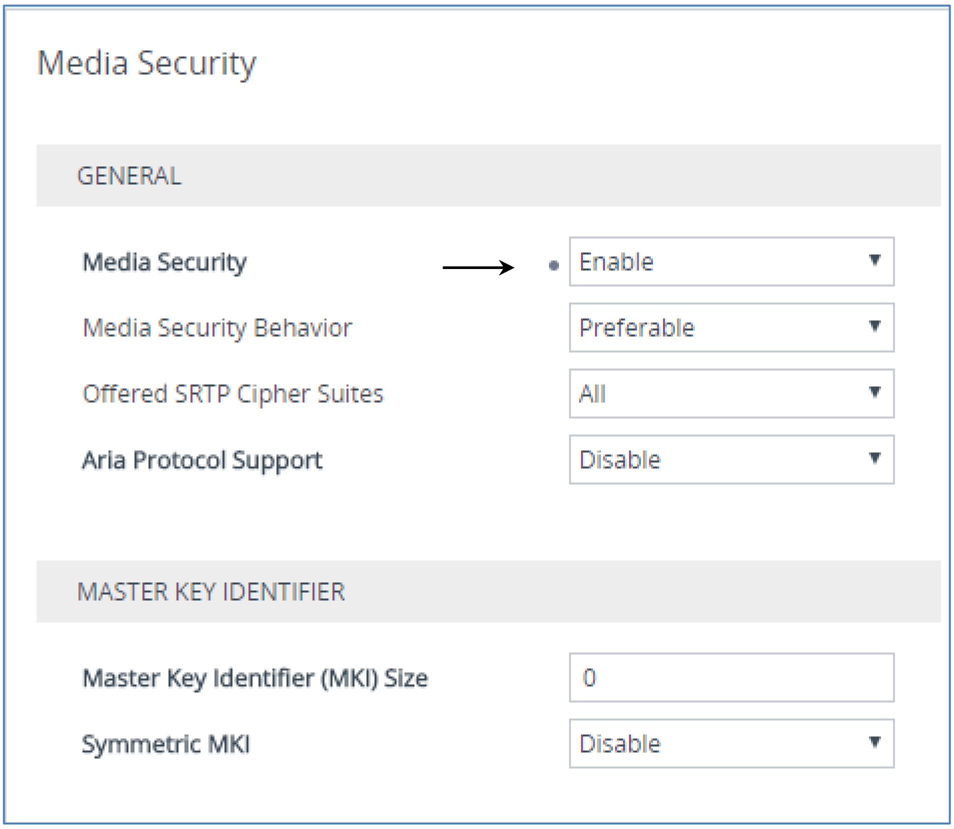
4.9 Configure SRTP (Optional)

This step describes how to configure media security. If the Generic SIP Trunk or AWS Chime Voice Connector requires SRTP, configure the SBC to operate in the same manner. Note that SRTP is enabled for these entities when you configure an IP Profile (see Section 4.5 on page 23).

➢ **To configure media security:**

1. Open the Media Security page (**Setup menu > Signaling & Media tab > Media folder > Media Security**).

Figure 4-18: Configuring SRTP



2. From the 'Media Security' drop-down list, select **Enable** to enable SRTP.
3. Click **Apply**.

4.10 Configure IP-to-IP Call Routing Rules

This section describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between AWS Chime Voice Connector and Generic SIP Trunk:

- Terminate SIP OPTIONS messages on the SBC that are received from any entity
- Calls from IP-PBX to Generic SIP Trunk
- Calls from Generic SIP Trunk to IP-PBX

➢ **To configure IP-to-IP routing rules:**

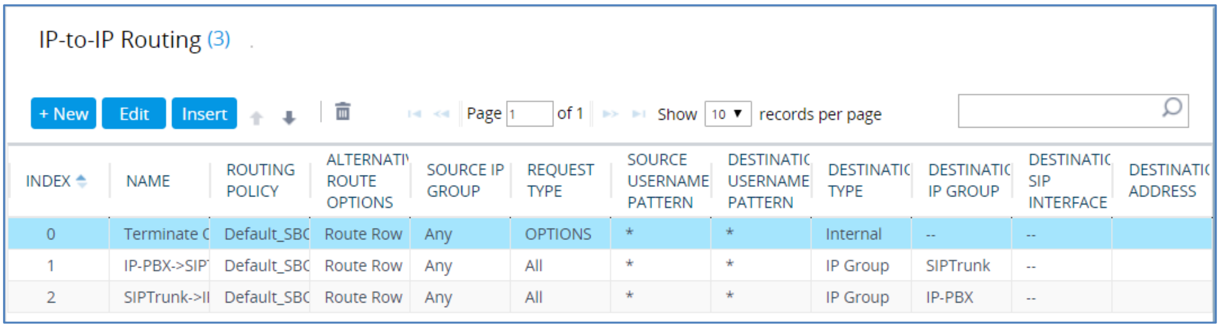
1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Configure routing rules as shown in the table below:

Table 4-8: Configuration IP-to-IP Routing Rules

Index	Name	Source IP Group	Request Type	Dest Type	Dest IP Group	Internal Action
0	Terminate OPTIONS	Any	OPTIONS	Internal		Reply(Response='200')
1	IP-PBX->SIPTrunk (arbitrary name)	IP-PBX		IP Group	SIPTrunk	
2	SIPTrunk->IP-PBX (arbitrary name)	SIPTrunk		IP Group	IP-PBX	

The configured routing rules are shown in the figure below:

Figure 4-19: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table



Note: The routing configuration may change according to your specific deployment topology.

4.11 Configuring SIP Recording

This section describes SBC's SIP Recording configuration.

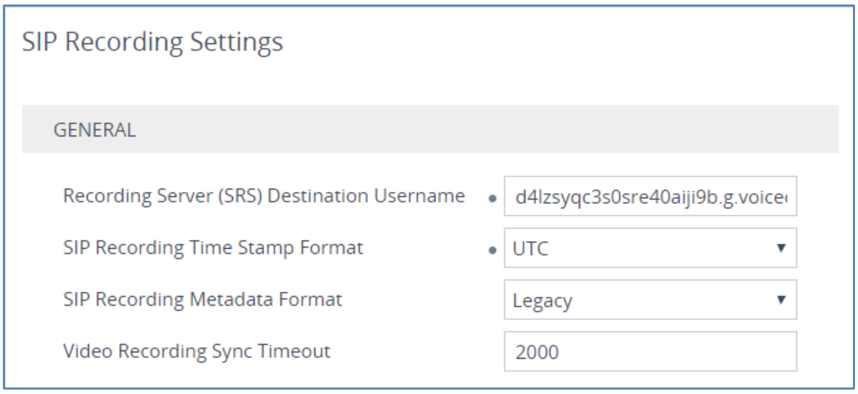
4.11.1 Configuring SIP Recording Settings

This section describes how to configure general SIP Recording settings.

➢ **To configure general SIP Recording Settings:**

1. Open the SIP Recording Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Recording** folder > **SIP Recording Settings**).

Figure 4-20: SIP Recording General Settings



2. In the 'Recording Server (SRS) Destination Username**'** field, enter a user part value according to AWS Chime Voice Connector requirement (for example, **d4lzsyqc3s0sre40aiji9b.g.voiceconnector.chime.aws**).
3. From the 'SIP Recording Time Stamp Format' drop-down list, select **UTC**.
4. From the 'SIP Recording Metadata Format' drop-down list, select **Legacy**.
5. Click **Apply**, and then save your settings to flash memory.

4.11.2 Configuring SIP Recording Rules

This section describes how to configure SIP Recording rules through the Web interface. The SIP Recording Rules table lets you configure up to 30 SIP-based media recording rules. A SIP Recording rule defines call routes that you want to record.

➢ **To configure a SIP Recording Routing rule:**

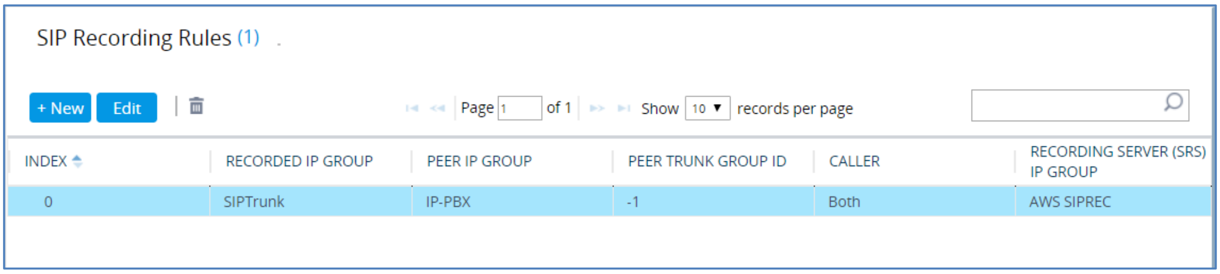
1. Open the SIP Recording Rules table (**Setup** menu > **Signaling & Media** tab > **SIP Recording** folder > **SIP Recording Rules**).
2. Click **New** and configure a SIP recording rule according to the table below:

Table 4-9: SIP Recording Rule

Index	Recorded IP Group	Peer IP Group	Caller	Recording Server (SRS) IP Group
0	SIPTrunk	IP-PBX	Both	AWS SIPREC

The configured SIP recording rules are shown in the figure below:

Figure 4-21: Configured SIP Recording Rules



SIP Recording Rules (1)

+ New | Edit | Page 1 of 1 | Show 10 records per page

INDEX	RECORDED IP GROUP	PEER IP GROUP	PEER TRUNK GROUP ID	CALLER	RECORDING SERVER (SRS) IP GROUP
0	SIPTrunk	IP-PBX	-1	Both	AWS SIPREC

4.12 Configure Number Manipulation Rules (Optional)

IP-to-IP manipulation rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Section 4.7 on page 22) to denote the source and destination of the call.

Note: Configure Number Manipulation Rules only if this is required by the SIP Trunk. For a detailed description, refer to the Configuration Notes document for the specific SIP Trunk.

4.13 Configure Message Manipulation Rules (Optional)

This section describes how to configure SIP message manipulation rules. SIP message manipulation rules can include insertion, removal, and/or modification of SIP headers. Manipulation rules are grouped into Manipulation Sets, enabling you to apply multiple rules to the same SIP message (IP entity).

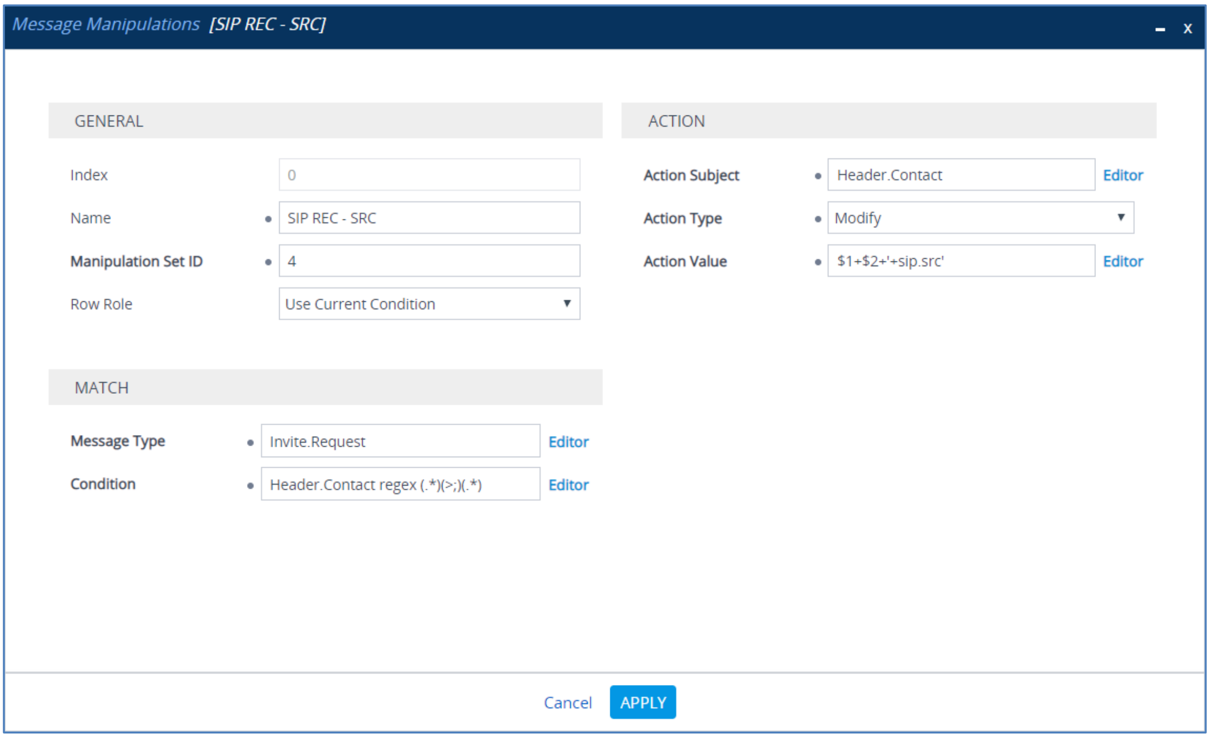
Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

➢ **To configure SIP message manipulation rule:**

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Configure a manipulation rule (Manipulation Set 4) for the AWS Chime Voice Connector SIPREC service. This rule applies to messages sent to the AWS SIPREC service. This adds a string ‘sip.src’ to the SIP Contact Header.

Parameter	Value
Index	**0**
Name	**SIP REC - SRC**
Manipulation Set ID	**4**
Message Type	**Invite.Request**
Condition	**Header.Contact regex (.*)(>;)(.*)**
Action Subject	**Header.Contact**
Action Type	**Modify**
Action Value	**$1+$2+'+sip.src'**

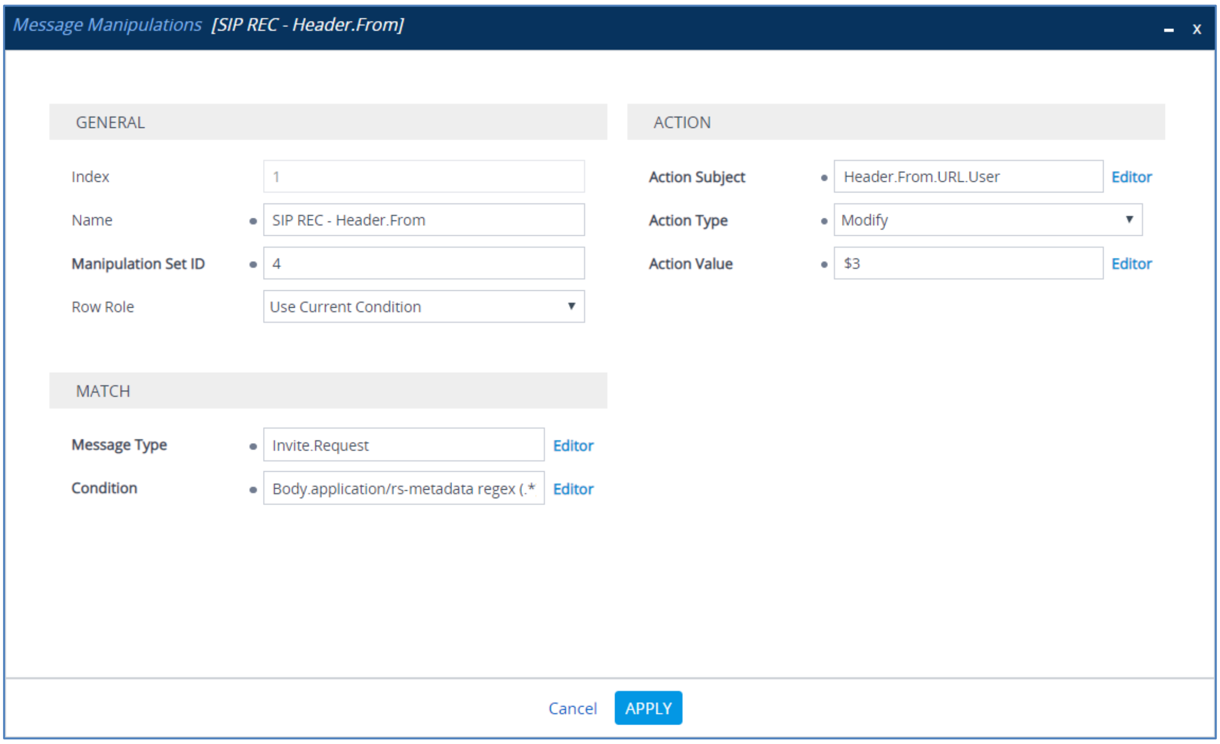
Figure 4-22: Configuring SIP Message Manipulation Rule 0 (for AWS SIPREC)



3. Configure another manipulation rule (Manipulation Set 4) for the AWS Chime Voice Connector SIPREC service. This rule applies to messages sent to the AWS SIPREC service. This modifies the user part of the SIP From header with the name, extracted from the metadata.

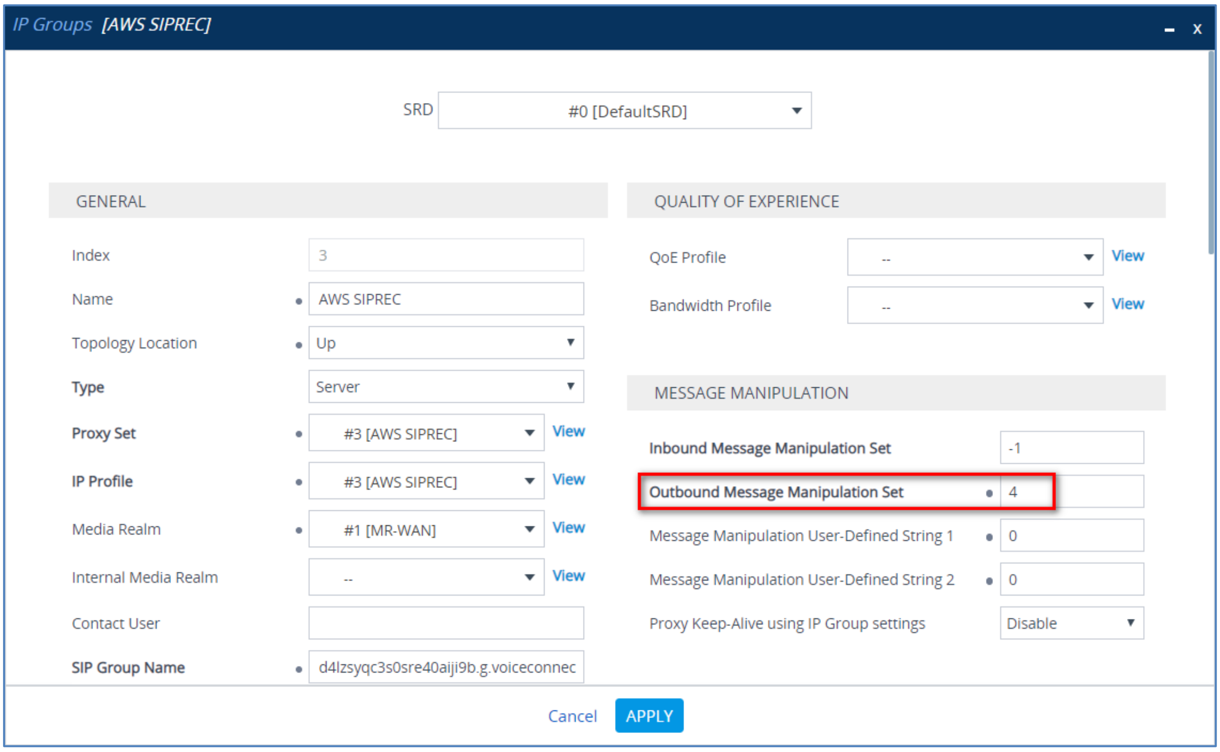
Parameter	Value
Index	**1**
Name	**SIP REC - Header.From**
Manipulation Set ID	**4**
Message Type	**Invite.Request**
Condition	**Body.application/rs-metadata regex (.*)(<nameID aor=")(.*)(@)(.*)(<nameID aor=")(.*)**
Action Subject	**Header.From.URL.User**
Action Type	**Modify**
Action Value	**$3**

Figure 4-23: Configuring SIP Message Manipulation Rule 1 (for AWS SIPREC)



4. Assign Manipulation Set ID 4 to the AWS SIPREC IP Group:
   a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
   b. Select the row of the AWS SIPREC IP Group, and then click **Edit**.
   c. Set the 'Outbound Message Manipulation Set' field to **4**.

Figure 4-24: Assigning Manipulation Set 4 to the AWS SIPREC IP Group



   d. Click **Apply**, and then save your settings to flash memory.

Note: Configure additional Message Manipulation Rules only if this is required by the SIP Trunk. For a detailed description, refer to the Configuration Notes document for the specific SIP Trunk.

4.14 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

4.14.1 Configure Gateway Name for Sending in OPTIONS

This section describes how to configure the SBC to send its string name ("gateway name") in keep-alive SIP OPTIONS messages (host part of the Request-URI).

➢ **To configure Gateway Name:**

1. Open the Proxy & Registration page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** > **Proxy & Registration**).
2. Configure 'Gateway Name' (for example, **d4lzsyqc3s0sre40aiji9b.g.voiceconnector.chime.aws**).
3. From the 'Use Gateway Name for OPTIONS' drop-down list, select **Yes**.

Figure 4-25: Configuring Gateway Name

4. Click **Apply**, and then save your settings to flash memory.

4.14.2 Optimizing CPU Cores Usage for a Specific Service (relevant for Mediant 9000 and Software SBC only)

This section describes how to optimize the SBC's CPU cores usage for a specified profile to achieve maximum capacity for that profile. The supported profiles include:

- SIP profile – improves SIP signaling performance, for example, SIP calls per second (CPS)
- SRTP profile – improves maximum number of SRTP sessions
- Transcoding profile – enables all DSP-required features, for example, transcoding and voice in-band detectors

➢ **To optimize core allocation for a profile:**

1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).
2. From the 'SBC Performance Profile' drop-down list, select the required profile:

3. Click **Apply**, and then reset the device with a burn-to-flash for your settings to take effect.

This page is intentionally left blank.

A AudioCodes INI File

The *ini* configuration file of the SBC, corresponding to the Web-based configuration as described in Section 4 on page 15, is shown below:

> **Note:** To load or save an *ini* file, use the Configuration File page (**Setup** menu > **Administration** tab > **Maintenance** folder > **Configuration File**).

```
;**************
;** Ini File **
;**************

[SYSTEM Params]

SyslogServerIP = 10.13.2.5
EnableSyslog = 0
NTPServerUTCOffset = 7200
ENABLEPARAMETERSMONITORING = 1
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
NTPServerIP = '8.8.8.8'

[Voice Engine Params]

PLThresholdLevelsPerMille_0 = 5
PLThresholdLevelsPerMille_1 = 10
PLThresholdLevelsPerMille_2 = 20
PLThresholdLevelsPerMille_3 = 50
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

Languages = 'en-US', '', '', '', '', '', '', '', '', ''

[SIP Params]

GWDEBUGLEVEL = 5
SIPGATEWAYNAME = 'd4lzsyqc3s0sre40aiji9b.g.voiceconnector.chime.aws'
USEGATEWAYNAMEFOROPTIONS = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
SIPRECSERVERDESTUSERNAME =
'd4lzsyqc3s0sre40aiji9b.g.voiceconnector.chime.aws'
SIPRECTIMESTAMP = 1

[ DeviceTable ]

FORMAT Index = VlanID, UnderlyingInterface, DeviceName, Tagging, MTU;
DeviceTable 0 = 1, "GROUP_1", "vlan 1", 0, 1500;
DeviceTable 1 = 2, "GROUP_2", "vlan 2", 0, 1500;

[ \DeviceTable ]
```

```
[ InterfaceTable ]

FORMAT Index = ApplicationTypes, InterfaceMode, IPAddress, PrefixLength,
Gateway, InterfaceName, PrimaryDNSServerIPAddress,
SecondaryDNSServerIPAddress, UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.7.21, 16, 10.15.0.1, "LAN_IF", 0.0.0.0,
0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.149, 25, 195.189.192.129, "WAN_IF",
8.8.8.8, 0.0.0.0, "vlan 2";

[ \InterfaceTable ]


[ TLSContexts ]

FORMAT Index = Name, TLSVersion, DTLSVersion, ServerCipherString,
ClientCipherString, RequireStrictCert, TlsRenegotiation, OcspEnable,
OcspServerPrimary, OcspServerSecondary, OcspServerPort,
OcspDefaultResponse, DHKeySize;
TLSContexts 0 = "default", 0, 0, "DEFAULT", "DEFAULT", 0, 1, 0, 0.0.0.0,
0.0.0.0, 2560, 0, 1024;

[ \TLSContexts ]


[ AudioCodersGroups ]

FORMAT Index = Name;
AudioCodersGroups 0 = "AudioCodersGroups_0";

[ \AudioCodersGroups ]


[ IpProfile ]

FORMAT Index = ProfileName, IpPreference, CodersGroupName, IsFaxUsed,
JitterBufMinDelay, JitterBufOptFactor, IPDiffServ, SigIPDiffServ,
RTPRedundancyDepth, CNGmode, VxxTransportType, NSEMode, IsDTMFUsed,
PlayRBTone2IP, EnableEarlyMedia, ProgressIndicator2IP,
EnableEchoCanceller, CopyDest2RedirectNumber, MediaSecurityBehaviour,
CallLimit, DisconnectOnBrokenConnection, FirstTxDtmfOption,
SecondTxDtmfOption, RxDTMFOption, EnableHold, InputGain, VoiceVolume,
AddIEInSetup, SBCExtensionCodersGroupName, MediaIPVersionPreference,
TranscodingMode, SBCAllowedMediaTypes, SBCAllowedAudioCodersGroupName,
SBCAllowedVideoCodersGroupName, SBCAllowedCodersMode,
SBCMediaSecurityBehaviour, SBCRFC2833Behavior, SBCAlternativeDTMFMethod,
SBCSendMultipleDTMFMethods, SBCAssertIdentity,
AMDSensitivityParameterSuit, AMDSensitivityLevel, AMDMaxGreetingTime,
AMDMaxPostSilenceGreetingTime, SBCDiversionMode, SBCHistoryInfoMode,
EnableQSIGTunneling, SBCFaxCodersGroupName, SBCFaxBehavior,
SBCFaxOfferMode, SBCFaxAnswerMode, SbcPrackMode, SBCSessionExpiresMode,
SBCRemoteUpdateSupport, SBCRemoteReinviteSupport,
SBCRemoteDelayedOfferSupport, SBCRemoteReferBehavior,
SBCRemote3xxBehavior, SBCRemoteMultiple18xSupport,
SBCRemoteEarlyMediaResponseType, SBCRemoteEarlyMediaSupport,
EnableSymmetricMKI, MKISize, SBCEnforceMKISize, SBCRemoteEarlyMediaRTP,
SBCRemoteSupportsRFC3960, SBCRemoteCanPlayRingback, EnableEarly183,
EarlyAnswerTimeout, SBC2833DTMFPayloadType, SBCUserRegistrationTime,
ResetSRTPStateUponRekey, AmdMode, SBCReliableHeldToneSource,
```

```
GenerateSRTPKeys, SBCPlayHeldTone, SBCRemoteHoldFormat,
SBCRemoteReplacesBehavior, SBCSDPPtimeAnswer, SBCPreferredPTime,
SBCUseSilenceSupp, SBCRTPRedundancyBehavior, SBCPlayRBTToTransferee,
SBCRTCPMode, SBCJitterCompensation, SBCRemoteRenegotiateOnFaxDetection,
JitterBufMaxDelay, SBCUserBehindUdpNATRegistrationTime,
SBCUserBehindTcpNATRegistrationTime, SBCSDPHandleRTCPAttribute,
SBCRemoveCryptoLifetimeInSDP, SBCIceMode, SBCRTCPMux,
SBCMediaSecurityMethod, SBCHandleXDetect, SBCRTCPFeedback,
SBCRemoteRepresentationMode, SBCKeepVIAHeaders, SBCKeepRoutingHeaders,
SBCKeepUserAgentHeader, SBCRemoteMultipleEarlyDialogs,
SBCRemoteMultipleAnswersMode, SBCDirectMediaTag,
SBCAdaptRFC2833BWToVoiceCoderBW, CreatedByRoutingServer,
SBCFaxReroutingMode, SBCMaxCallDuration, SBCGenerateRTP,
SBCISUPBodyHandling, SBCISUPVariant, SBCVoiceQualityEnhancement,
SBCMaxOpusBW, SBCEnhancedPlc, LocalRingbackTone, LocalHeldTone,
SBCGenerateNoOp, SBCRemoveUnKnownCrypto, SBCMultipleCoders, DataDiffServ,
SBCMSRPReinviteUpdateSupport, SBCMSRPOfferSetupRole, SBCMSRPEmpMsg;
IpProfile 1 = "IP-PBX", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0,
0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "",
"AudioCodersGroups_0", 0, 0, "", "", "", 0, 0, 0, 0, 0, 0, 0, 8, 300,
400, 0, 0, 0, "", 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 300, -1, -1,
0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, -1, -1, 0, 0, 0, 0, 1, 2, 0;
IpProfile 2 = "SIPTrunk", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0,
0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "",
"AudioCodersGroups_0", 0, 0, "", "", "", 0, 0, 0, 0, 0, 0, 0, 8, 300,
400, 0, 0, 0, "", 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 300, -1, -1,
0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, -1, -1, 0, 0, 0, 0, 1, 2, 0;
IpProfile 3 = "AWS SIPREC", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24,
0, 0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "",
"AudioCodersGroups_0", 0, 0, "", "", "", 0, 2, 0, 0, 0, 0, 0, 8, 300,
400, 0, 0, 0, "", 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 300, -1, -1,
0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, -1, -1, 0, 0, 0, 0, 1, 2, 0;

[ \IpProfile ]


[ CpMediaRealm ]

FORMAT Index = MediaRealmName, IPv4IF, IPv6IF, RemoteIPv4IF,
RemoteIPv6IF, PortRangeStart, MediaSessionLeg, PortRangeEnd,
TCPPortRangeStart, TCPPortRangeEnd, IsDefault, QoeProfile, BWProfile,
TopologyLocation;
CpMediaRealm 0 = "MR-LAN", "LAN_IF", "", "", "", 6000, 100, 6999, 0, 0,
1, "", "", 0;
CpMediaRealm 1 = "MR-WAN", "WAN_IF", "", "", "", 50000, 100, 50999, 0, 0,
0, "", "", 1;

[ \CpMediaRealm ]


[ SBCRoutingPolicy ]

FORMAT Index = Name, LCREnable, LCRAverageCallLength, LCRDefaultCost,
LdapServerGroupName;
SBCRoutingPolicy 0 = "Default_SBCRoutingPolicy", 0, 1, 0, "";

[ \SBCRoutingPolicy ]
```

```
[ SRD ]

FORMAT Index = Name, BlockUnRegUsers, MaxNumOfRegUsers,
EnableUnAuthenticatedRegistrations, SharingPolicy, UsedByRoutingServer,
SBCOperationMode, SBCRoutingPolicyName, SBCDialPlanName,
AdmissionProfile;
SRD 0 = "DefaultSRD", 0, -1, 1, 0, 0, 0, "Default_SBCRoutingPolicy", "",
"";

[ \SRD ]


[ MessagePolicy ]

FORMAT Index = Name, MaxMessageLength, MaxHeaderLength, MaxBodyLength,
MaxNumHeaders, MaxNumBodies, SendRejection, MethodList, MethodListType,
BodyList, BodyListType, UseMaliciousSignatureDB;
MessagePolicy 0 = "Malicious Signature DB Protection", -1, -1, -1, -1, -
1, 1, "", 0, "", 0, 1;

[ \MessagePolicy ]


[ SIPInterface ]

FORMAT Index = InterfaceName, NetworkInterface,
SCTPSecondaryNetworkInterface, ApplicationType, UDPPort, TCPPort,
TLSPort, SCTPPort, AdditionalUDPPorts, AdditionalUDPPortsMode, SRDName,
MessagePolicyName, TLSContext, TLSMutualAuthentication,
TCPKeepaliveEnable, ClassificationFailureResponseType,
PreClassificationManSet, EncapsulatingProtocol, MediaRealm,
SBCDirectMedia, BlockUnRegUsers, MaxNumOfRegUsers,
EnableUnAuthenticatedRegistrations, UsedByRoutingServer,
TopologyLocation, PreParsingManSetName, AdmissionProfile,
CallSetupRulesSetId;
SIPInterface 0 = "Int-LAN", "LAN_IF", "", 2, 5060, 5070, 0, 0, "", 0,
"DefaultSRD", "Malicious Signature DB Protection", "default", -1, 0, 500,
-1, 0, "MR-LAN", 0, -1, -1, -1, 0, 0, "", "", -1;
SIPInterface 1 = "Int-WAN", "WAN_IF", "", 2, 5060, 5060, 5061, 0, "", 0,
"DefaultSRD", "Malicious Signature DB Protection", "default", -1, 0, 500,
-1, 0, "MR-WAN", 0, -1, -1, -1, 0, 1, "", "", -1;

[ \SIPInterface ]


[ ProxySet ]

FORMAT Index = ProxyName, EnableProxyKeepAlive, ProxyKeepAliveTime,
ProxyLoadBalancingMethod, IsProxyHotSwap, SRDName, ClassificationInput,
TLSContextName, ProxyRedundancyMode, DNSResolveMethod,
KeepAliveFailureResp, GWIPv4SIPInterfaceName, SBCIPv4SIPInterfaceName,
GWIPv6SIPInterfaceName, SBCIPv6SIPInterfaceName, MinActiveServersLB,
SuccessDetectionRetries, SuccessDetectionInterval,
FailureDetectionRetransmissions;
ProxySet 0 = "ProxySet_0", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "",
"", "Int-LAN", "", "", 1, 1, 10, -1;
ProxySet 1 = "IP-PBX", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"Int-LAN", "", "", 1, 1, 10, -1;
```

```
ProxySet 2 = "SIPTrunk", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "", "Int-WAN", "", "", 1, 1, 10, -1;
ProxySet 3 = "AWS SIPREC", 1, 60, 0, 1, "DefaultSRD", 0, "", -1, -1, "", "", "Int-WAN", "", "", 1, 1, 10, -1;

[ \ProxySet ]


[ IPGroup ]

FORMAT Index = Type, Name, ProxySetName, SIPGroupName, ContactUser, SipReRoutingMode, AlwaysUseRouteTable, SRDName, MediaRealm, InternalMediaRealm, ClassifyByProxySet, ProfileName, MaxNumOfRegUsers, InboundManSet, OutboundManSet, RegistrationMode, AuthenticationMode, MethodList, SBCServerAuthType, OAuthHTTPService, EnableSBCClientForking, SourceUriInput, DestUriInput, ContactName, Username, Password, UUIFormat, QOEProfile, BWProfile, AlwaysUseSourceAddr, MsgManUserDef1, MsgManUserDef2, SIPConnect, SBCPSAPMode, DTLSContext, CreatedByRoutingServer, UsedByRoutingServer, SBCOperationMode, SBCRouteUsingRequestURIPort, SBCKeepOriginalCallID, TopologyLocation, SBCDialPlanName, CallSetupRulesSetId, Tags, SBCUserStickiness, UserUDPPortAssignment, AdmissionProfile, ProxyKeepAliveUsingIPG, SBCAltRouteReasonsSetName, TeamsMediaOptimization;
IPGroup 0 = 0, "Default_IPG", "ProxySet_0", "", "", -1, 0, "DefaultSRD", "MR-LAN", "", 1, "", -1, -1, -1, 0, 0, "", -1, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", 0, "0", "0", 0, 0, "default", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0, "", 0, "", 0;
IPGroup 1 = 0, "IP-PBX", "IP-PBX", "d4lzsyqc3s0sre40aiji9b.g.voiceconnector.chime.aws", "", -1, 0, "DefaultSRD", "MR-LAN", "", 1, "IP-PBX", -1, -1, -1, 0, 0, "", -1, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", 0, "0", "0", 0, 0, "default", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0, "", 0, "", 0;
IPGroup 2 = 0, "SIPTrunk", "SIPTrunk", "d4lzsyqc3s0sre40aiji9b.g.voiceconnector.chime.aws", "", -1, 0, "DefaultSRD", "MR-LAN", "", 1, "SIPTrunk", -1, -1, -1, 0, 0, "", -1, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", 0, "0", "0", 0, 0, "default", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0, "", 0, "", 0;
IPGroup 3 = 0, "AWS SIPREC", "AWS SIPREC", "d4lzsyqc3s0sre40aiji9b.g.voiceconnector.chime.aws", "", -1, 0, "DefaultSRD", "MR-WAN", "", 1, "AWS SIPREC", -1, -1, 4, 0, 0, "", -1, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", 0, "0", "0", 0, 0, "default", 0, 0, -1, 0, 0, 1, "", -1, "", 0, 0, "", 0, "", 0;

[ \IPGroup ]


[ ProxyIp ]

FORMAT Index = ProxySetId, ProxyIpIndex, IpAddress, TransportType, Priority, Weight;
ProxyIp 1 = "1", 0, "10.10.10.10:5060", 0, 0, 0;
ProxyIp 2 = "2", 0, "SIPTrunk.com:5060", 0, 0, 0;
ProxyIp 3 = "3", 0, "d4lzsyqc3s0sre40aiji9b.g.voiceconnector.chime.aws:5060", 0, 0, 0;

[ \ProxyIp ]


[ IP2IPRouting ]

FORMAT Index = RouteName, RoutingPolicyName, SrcIPGroupName, SrcUsernamePrefix, SrcHost, DestUsernamePrefix, DestHost, RequestType,
```

```
MessageConditionName, ReRouteIPGroupName, Trigger, CallSetupRulesSetId,
DestType, DestIPGroupName, DestSIPInterfaceName, DestAddress, DestPort,
DestTransportType, AltRouteOptions, GroupPolicy, CostGroup, DestTags,
SrcTags, IPGroupSetName, RoutingTagName, InternalAction;
IP2IPRouting 0 = "Terminate OPTIONS", "Default_SBCRoutingPolicy", "Any",
"*", "*", "*", "*", 6, "", "Any", 0, -1, 13, "", "", "", 0, -1, 0, 0, "",
"", "", "", "default", "Reply(Response='200')";
IP2IPRouting 1 = "IP-PBX->SIPTrunk", "Default_SBCRoutingPolicy", "Any",
"*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "SIPTrunk", "", "", 0, -1, 0,
0, "", "", "", "", "default", "";
IP2IPRouting 2 = "SIPTrunk->IP-PBX", "Default_SBCRoutingPolicy", "Any",
"*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "IP-PBX", "", "", 0, -1, 0,
0, "", "", "", "", "default", "";

[ \IP2IPRouting ]


[ MessageManipulations ]

FORMAT Index = ManipulationName, ManSetID, MessageType, Condition,
ActionSubject, ActionType, ActionValue, RowRole;
MessageManipulations 0 = "SIP REC - SRC", 4, "Invite.Request",
"Header.Contact regex (.*)(>;)(.*)", "Header.Contact", 2,
"$1+$2+'+sip.src'", 0;
MessageManipulations 1 = "SIP REC - Header.From", 4, "Invite.Request",
'Body.application/rs-metadata regex (.*)(<nameID
aor=")(.*)(@)(.*)(<nameID aor=")(.*)', "Header.From.URL.User", 2, "$3",
0;

[ \MessageManipulations ]


[ GwRoutingPolicy ]

FORMAT Index = Name, LCREnable, LCRAverageCallLength, LCRDefaultCost,
LdapServerGroupName;
GwRoutingPolicy 0 = "GwRoutingPolicy", 0, 1, 0, "";

[ \GwRoutingPolicy ]


[ ResourcePriorityNetworkDomains ]

FORMAT Index = Name, Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 1;
ResourcePriorityNetworkDomains 2 = "dod", 1;
ResourcePriorityNetworkDomains 3 = "drsn", 1;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 1;

[ \ResourcePriorityNetworkDomains ]


[ SIPRecRouting ]

FORMAT Index = RecordedIPGroupName, RecordedSourcePrefix,
RecordedDestinationPrefix, ConditionName, PeerIPGroupName,
PeerTrunkGroupID, Caller, SRSIPGroupName, SRSRedundantIPGroupName;
```

```
SIPRecRouting 0 = "SIPTrunk", "*", "*", "", "IP-PBX", -1, 0, "AWS
SIPREC", "";

[ \SIPRecRouting ]


[ MaliciousSignatureDB ]

FORMAT Index = Name, Pattern;
MaliciousSignatureDB 0 = "SIPVicious", "Header.User-Agent.content prefix
'friendly-scanner'";
MaliciousSignatureDB 1 = "SIPScan", "Header.User-Agent.content prefix
'sip-scan'";
MaliciousSignatureDB 2 = "Smap", "Header.User-Agent.content prefix
'smap'";
MaliciousSignatureDB 3 = "Sipsak", "Header.User-Agent.content prefix
'sipsak'";
MaliciousSignatureDB 4 = "Sipcli", "Header.User-Agent.content prefix
'sipcli'";
MaliciousSignatureDB 5 = "Sivus", "Header.User-Agent.content prefix
'SIVuS'";
MaliciousSignatureDB 6 = "Gulp", "Header.User-Agent.content prefix
'Gulp'";
MaliciousSignatureDB 7 = "Sipv", "Header.User-Agent.content prefix
'sipv'";
MaliciousSignatureDB 8 = "Sundayddr Worm", "Header.User-Agent.content
prefix 'sundayddr'";
MaliciousSignatureDB 9 = "VaxIPUserAgent", "Header.User-Agent.content
prefix 'VaxIPUserAgent'";
MaliciousSignatureDB 10 = "VaxSIPUserAgent", "Header.User-Agent.content
prefix 'VaxSIPUserAgent'";
MaliciousSignatureDB 11 = "SipArmyKnife", "Header.User-Agent.content
prefix 'siparmyknife'";

[ \MaliciousSignatureDB ]


[ AudioCoders ]

FORMAT Index = AudioCodersGroupId, AudioCodersIndex, Name, pTime, rate,
PayloadType, Sce, CoderSpecific;
AudioCoders 0 = "AudioCodersGroups_0", 0, 2, 2, 90, -1, 0, "";

[ \AudioCoders ]
```

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
200 Cottontail Lane
Suite A101E
Somerset NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
website: https://www.audiocodes.com

Document #: LTRT-29325