

Mediant™ E-SBC for Mediant CCE Appliance and ITSP SIP Trunk

Version 7.2



Microsoft Partner

Gold Communications



Table of Contents

1	Introduction	7
1.1	Intended Audience	7
1.2	About AudioCodes E-SBC Product Series.....	7
2	Component Information.....	9
2.1	AudioCodes E-SBC Version	9
2.2	Microsoft Skype for Business CCE Version	9
2.3	Deploying the SBC	10
2.3.1	Example Environment.....	10
2.3.2	Environment Setup	11
3	Configuring Skype for Business CCE	13
3.1	Setting the SBC Certificate on the CCE.....	13
4	Configuring AudioCodes E-SBC.....	15
4.1	Step 1: IP Network Interfaces Configuration	16
4.1.1	Step 1a: Configure VLANs.....	17
4.1.2	Step 1b: Configure IP Network Interfaces for LAN and WAN	18
4.2	Step 2: Enable the SBC Application	19
4.3	Step 3: Configure Media Realms.....	20
4.4	Step 4: Configure SIP Signaling Interfaces.....	23
4.5	Step 5: Configure Proxy Sets	25
4.6	Step 6: Configure Coders	28
4.7	Step 7: Configure IP Profiles	31
4.8	Step 8: Configure IP Groups.....	35
4.9	Step 9: SIP TLS Connection Configuration	37
4.9.1	Step 9a: Configure the NTP Server Address.....	37
4.9.2	Step 9b: Configure the TLS version	38
4.9.3	Step 9c: Configure a Certificate.....	39
4.10	Step 10: Configure SRTP	40
4.11	Step 11: Configure Maximum IP Media Channels	41
4.12	Step 12: Configure IP-to-IP Call Routing Rules	42
4.13	Step 13: Configure IP-to-IP Manipulation Rules.....	47
4.14	Step 14: Configure Message Manipulation Rules	49
4.15	Step 15: Configure Registration Accounts	51
4.16	Step 16: Miscellaneous Configuration.....	52
4.16.1	Step 16a: Configure Call Forking Mode	52
4.16.2	Step 16b: Configure SBC Alternative Routing Reasons	53
4.17	Step 17: Reset the E-SBC	54

This page is intentionally left blank.

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published, nor can it accept responsibility for errors or omissions. Updates to this document and other documents as well as software files can be viewed by registered customers at <http://www.audiocodes.com/downloads>.

This document is subject to change without notice.

Date Published: April-09-2017

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 Web site at www.audiocodes.com/support.

Document Revision Record

LTRT	Description
28160	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://www.audiocodes.com/downloads>.

This page is intentionally left blank.

1 Introduction

This Configuration Note describes how to set up AudioCodes Enterprise Session Border Controller (hereafter, referred to as *E-SBC*) for interworking between ITSP's SIP Trunk and AudioCodes Mediant CCE Appliance.

You can also use AudioCodes' SBC Wizard tool to automatically configure the E-SBC based on this interoperability setup. However, it is recommended to read through this document in order to better understand the various configuration options. For more information on AudioCodes' SBC Wizard including download option, visit AudioCodes Web site at <http://www.audiocodes.com/sbc-wizard> (login required).

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and ITSP Partners who are responsible for installing and configuring ITSP's SIP Trunk and Microsoft's Skype for Business CCE for enabling VoIP calls using AudioCodes E-SBC.

1.2 About AudioCodes E-SBC Product Series

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

The E-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 E-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 E-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.

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	<ul style="list-style-type: none">▪ Mediant 800B Gateway & E-SBC▪ Mediant Software SBC (VE)
Software Version	SIP_7.20A or later
Protocol	<ul style="list-style-type: none">▪ SIP/UDP (to the ITSP SIP Trunk)▪ SIP/TCP or TLS (to the S4B Mediation Server)
Additional Notes	The Mediant CCE appliance is delivered with M800 SBC or SSBC in HP server.

2.2 Mediant CCE Appliance Version

Table 2-2: Microsoft Skype for Business CCE Version

Vendor	AudioCodes
Model	Mediant CCE Appliance
Software Version	Release 2.0.2
Protocol	SIP
Additional Notes	None

2.3 Microsoft Skype for Business Cloud Connector Edition Version

Table 2-3: Microsoft Skype for Business CCE Version

Vendor	Microsoft
Model	Cloud Connector Edition
Software Version	Release 1.4.2

2.4 Deploying the SBC

2.4.1 Example Environment

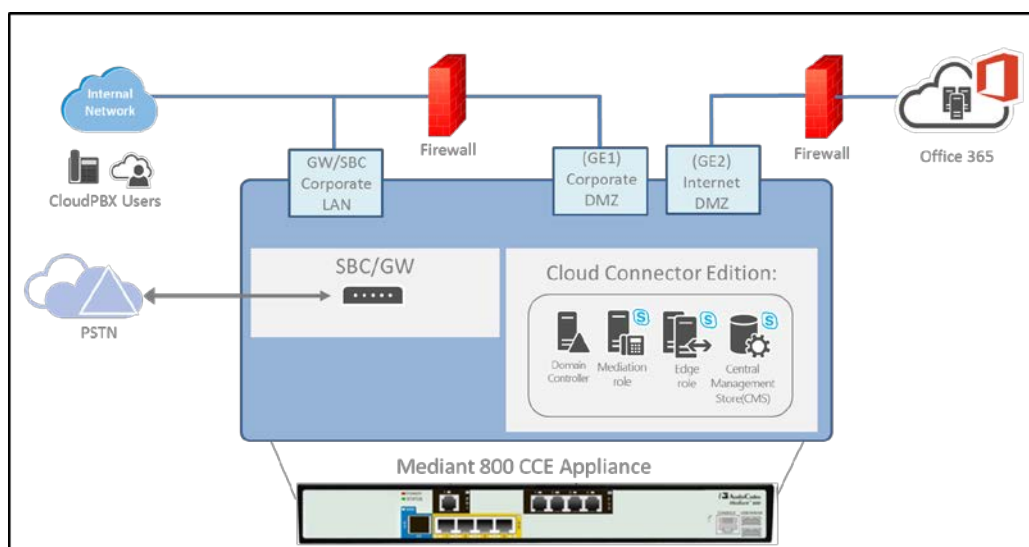
The example scenario below is referred to throughout this document in order to show how to deploy the SBC.

In the example environment:

- Enterprise deployed the Mediant CCE Appliance in its network for enhanced communication within the Cloud PBX.
- Enterprise wishes to offer its employees to connect the Enterprise to the Local PSTN network using ITSP's SIP Trunking service.
- AudioCodes E-SBC is implemented to interconnect between the CCE and the SIP Trunk.
 - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
 - **Border:** IP-to-IP network border between Mediant CCE network in the Enterprise LAN and ITSP's SIP Trunk located in the public network.

The figure below illustrates this interoperability test topology:

Figure 2-1: Example Environment Topology between E-SBC and Mediant CCE with ITSP SIP Trunk



2.4.2 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	<ul style="list-style-type: none">▪ CCE Mediation is located on the Corporate DMZ▪ ITSP SIP Trunk is located on the Internet DMZ
Signaling Transcoding	<ul style="list-style-type: none">▪ CCE operates with SIP-over-TLS transport type▪ ITSP SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	<ul style="list-style-type: none">▪ CCE supports G.711A-law and G.711U-law coders▪ ITSP SIP Trunk supports G.711A-law, G.711U-law, and G.729 coder
Media Transcoding	<ul style="list-style-type: none">▪ CCE operates with SRTP media type▪ ITSP SIP Trunk operates with RTP media type

This page is intentionally left blank.

3 Configuring Skype for Business CCE

This chapter describes how to configure Mediant CCE Appliance to assign certificate to the AudioCodes E-SBC.



Note: Other Settings on Cloud Connector Edition (CCE) are beyond the scope of this document. Refer to *LTRT-28086 Mediant Appliance for Microsoft Skype for Business CCE Installation Manual Ver. 2.0.2*.

3.1 Setting the SBC Certificate on the CCE

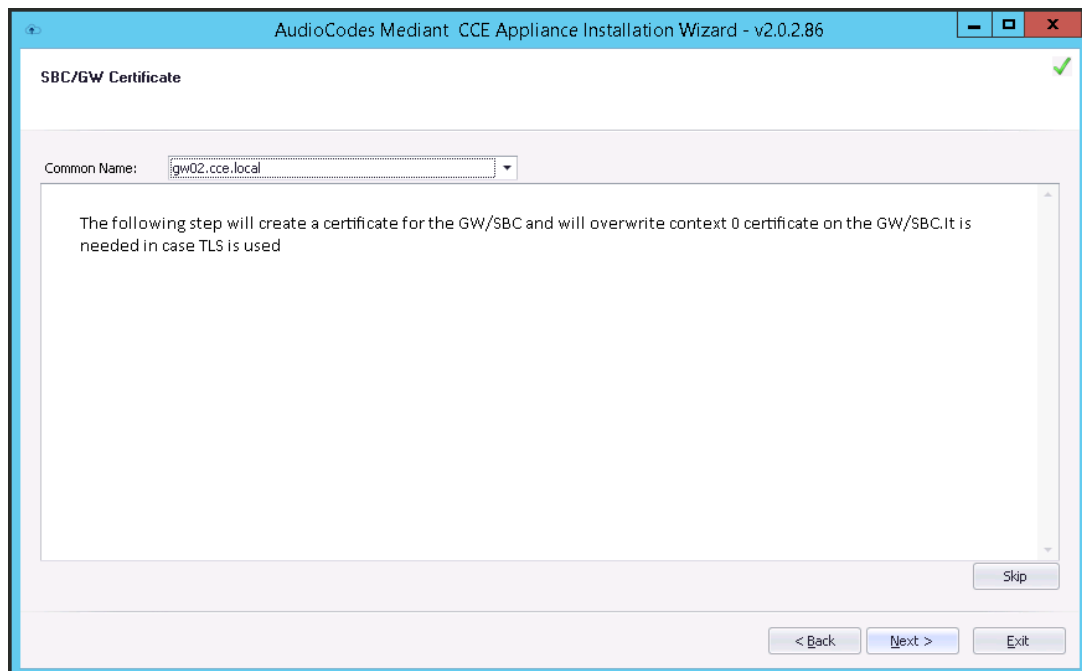
This procedure describes how to set the collocated SBC certificate. This certificate is required in case TLS is used to secure the connection between the Gateway/SBC and the CCE Mediation server.

The new certificate will be signed by the CCE internal CA automatically and be uploaded to the Gateway/SBC under Context index 0 (note: the new certificate will override any other certificate in context 0).

➤ **To set the SBC certificate:**

1. Select the correct SBC FQDN from the Common Name field. as shown below:

Figure 3-1: setting the SBC certificate



2. Click the **Next** button to continue.



Note: To deploy the certificate, ensure that the CCE has access to the SBC OSN IP (i.e., 169.254.100.1). The SBC is set with the parameter `OSNINTERNALVLAN=1`.

This page is intentionally left blank.

4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between Mediant CCE Appliance and the ITSP SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4.

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



Notes:

- For implementing Microsoft Skype for Business and ITSP SIP Trunk based on the configuration described in this section, AudioCodes E-SBC must be installed with a License Key that includes the following software features:

- ✓ **Microsoft**
- ✓ **SBC**
- ✓ **Security**
- ✓ **DSP**
- ✓ **RTP**
- ✓ **SIP**

For more information about the License Key, contact your AudioCodes sales representative.

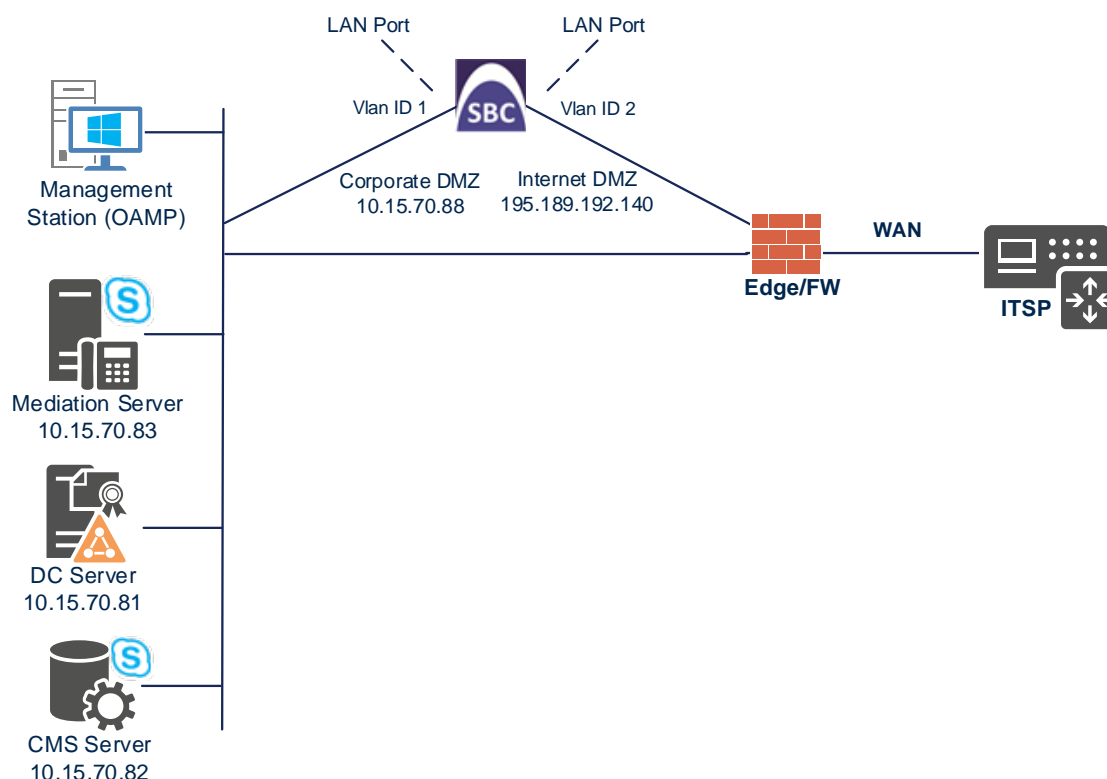
- The scope of this interoperability test and document does **not** cover all security aspects for connecting the SIP Trunk to the Microsoft Skype for Business environment. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document.

4.1 Step 1: IP Network Interfaces Configuration

This step describes how to configure the E-SBC's IP network interfaces. There are several ways to deploy the E-SBC; however, scenario exemplified in this document employs the following deployment method:

- E-SBC interfaces with the following IP entities:
 - CCE Mediation server, located on the Corporate DMZ
 - ITSP SIP Trunk, located on the Internet DMZ
- Physical connection: The type of physical connection to the Corporate depends on the method used to connect to the Enterprise's network. In this example, E-SBC connects to the Corporate DMZ and Internet DMZ using dedicated LAN ports (i.e., two ports and two network cables are used).
- E-SBC also uses two logical network interfaces:
 - Corporate DMZ (VLAN ID 1)
 - Internet DMZ (VLAN ID 2)

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 Step 1a: Configure VLANs

This step describes how to define VLANs for each of the following interfaces:

- Corporate DMZ VoIP (assigned the name "vlan 1")
- Internet DMZ VoIP (assigned the name "vlan 2")

➤ **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 as follows:

Parameter	Value
Index	1
VLAN ID	2
Underlying Interface	GROUP_2 (Ethernet port group)
Name	vlan 2
Tagging	Untagged

Figure 4-2: Configured VLAN IDs in Ethernet Device

Ethernet Devices (2)				
<div> + New Edit 🗑️ </div> <div> Page 1 of 1 Show 10 records per page </div>				
INDEX	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING
0	1	GROUP_1	vlan 1	Untagged
1	2	GROUP_2	vlan 2	Untagged

4.1.2 Step 1b: Configure IP Network Interfaces for LAN and WAN

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

- Corporate DMZ VoIP (assigned the name "LAN_IF")
- Internet DMZ VoIP (assigned the name "WAN_IF")

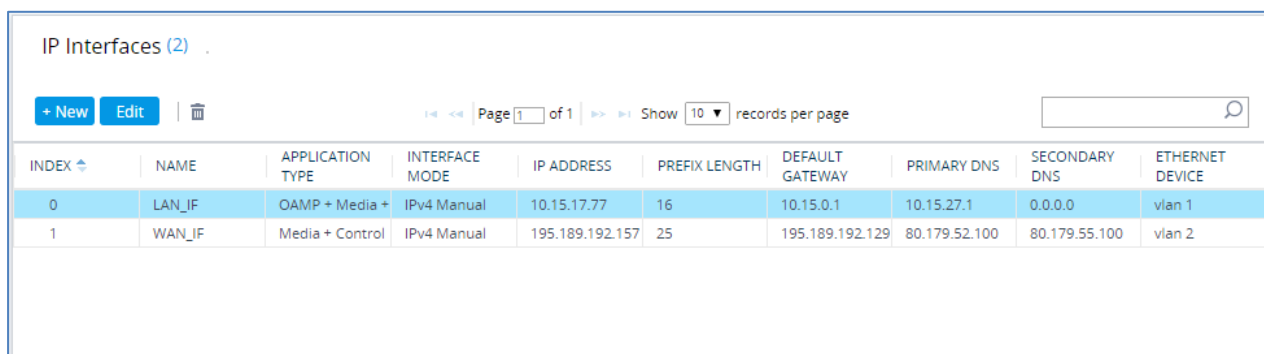
➤ **To configure the IP network interfaces:**

1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Configure the interface as follows:

IP Interface	Specific Configuration						
	Name	Application Type	IP Address	Prefix Length	Default Gateway	Primary DNS	Ethernet Device
Interfacing with Corporate DMZ	LAN_IF	OAMP + Media + Control	10.15.70.88	16	10.15.0.1	10.15.28.1	vlan 1
Interfacing with Internet DMZ	WAN_IF	Media + Control	195.189.192.141	25	195.189.192.129	8.8.8.8	vlan 2

3. Click **Apply**. The configured IP network interfaces are shown below:

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



<div> + New Edit </div> <div> Page 1 of 1 Show 10 records per page </div>									
INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	LAN_IF	OAMP + Media +	IPv4 Manual	10.15.17.77	16	10.15.0.1	10.15.27.1	0.0.0.0	vlan 1
1	WAN_IF	Media + Control	IPv4 Manual	195.189.192.157	25	195.189.192.129	80.179.52.100	80.179.55.100	vlan 2

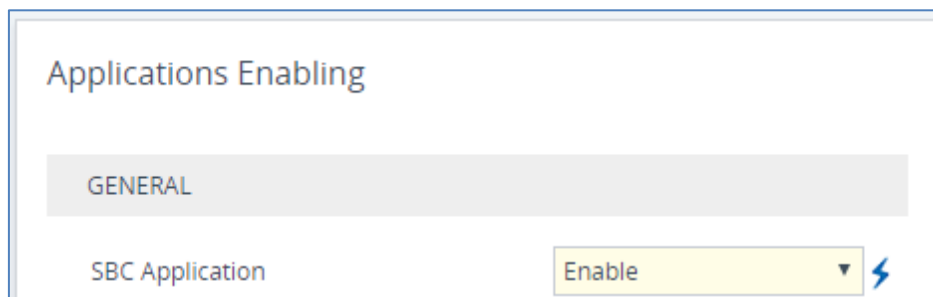
4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➤ **To enable the SBC application:**

1. Open the Applications Enabling page (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Applications Enabling**).

Figure 4-4: Enabling SBC Application



2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Apply**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.17 on page 54).

4.3 Step 3: Configure Media Realms

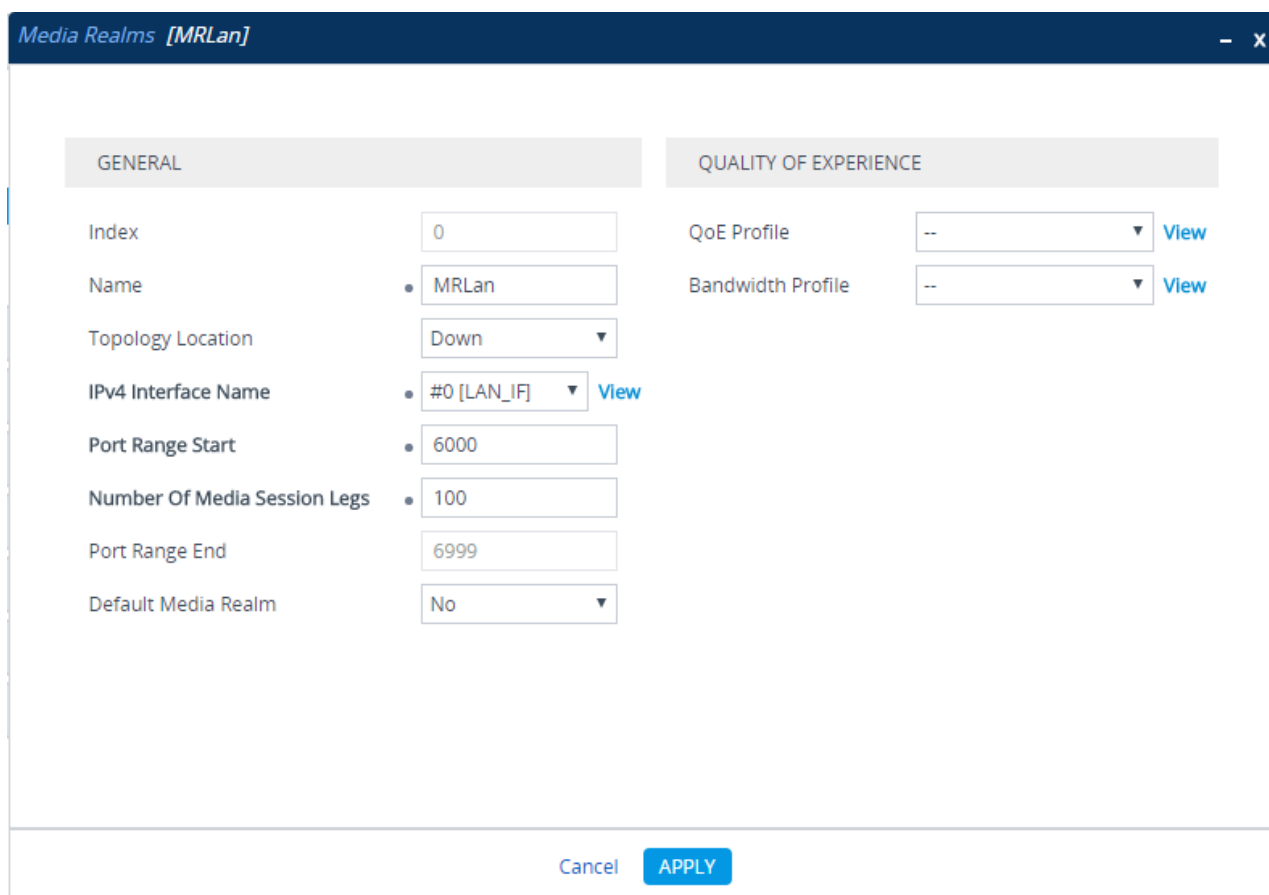
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➤ **To configure Media Realms:**

1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Add a Media Realm for the LAN interface. You can use the default Media Realm (Index 0), however modify it as shown below:

Parameter	Value
Index	0
Name	MRLan (descriptive name)
IPv4 Interface Name	LAN_IF
Port Range Start	6000 (represents lowest UDP port number used for media on LAN)
Number of Media Session Legs	100 (media sessions assigned with port range)

Figure 4-5: Configuring Media Realm for LAN



Media Realms [MRLan]

GENERAL

Index: 0

Name: MRLan

Topology Location: Down

IPv4 Interface Name: #0 [LAN_IF]

Port Range Start: 6000

Number Of Media Session Legs: 100

Port Range End: 6999

Default Media Realm: No

QUALITY OF EXPERIENCE

QoE Profile: --

Bandwidth Profile: --

Cancel APPLY

3. Configure a Media Realm for WAN traffic:

Parameter	Value
Index	1
Name	MRWan (arbitrary name)
Topology Location	Up
IPv4 Interface Name	WAN_IF
Port Range Start	7000 (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	100 (media sessions assigned with port range)

Figure 4-6: Configuring Media Realm for WAN

Media Realms [MRWan]

GENERAL

Index: 1

Name: • MRWan

Topology Location: • Up ▼

IPv4 Interface Name: • #1 [WAN_IF] ▼ [View](#)

Port Range Start: • 7000

Number Of Media Session Legs: • 100

Port Range End: 7999

Default Media Realm: No ▼

QUALITY OF EXPERIENCE

QoE Profile: -- ▼ [View](#)

Bandwidth Profile: -- ▼ [View](#)

Cancel [APPLY](#)

The configured Media Realms are shown in the figure below:

Figure 4-7: Configured Media Realms in Media Realm Table

Media Realms (2)

+ New Edit

Page 1 of 1

Show 10 records per page

INDEX	NAME	IPV4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	MRLan	LAN_IF	6000	100	6999	No
1	MRWan	WAN_IF	7000	100	7999	No

4.4 Step 4: Configure SIP Signaling Interfaces

This step describes how to configure SIP Interfaces. In the example scenario, an internal and external SIP Interface must be configured for the E-SBC.

➤ **To configure SIP Interfaces:**

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Add a SIP Interface for the LAN interface. You can use the default SIP Interface (Index 0), but modify it as shown below:

Parameter	Value
Index	0
Name	S4B (see note at the end of this section)
Network Interface	LAN_IF
Application Type	SBC
UDP and TCP	0
TLS Port	5067 (see note below)
Media Realm	MRLan



Note: The TLS port parameter must be identically as configured during the Mediant CCE installation using the CCE Install Wizard.

3. Configure a SIP Interface for the WAN:

Parameter	Value
Index	1
Name	ITSP
Network Interface	WAN_IF
Application Type	SBC
UDP Port	5060
TCP and TLS	0
Media Realm	MRWan

The configured SIP Interfaces are shown in the figure below:

Figure 4-8: Configured SIP Interfaces in SIP Interface Table

SIP Interfaces (2)

+ New Edit

Page 1 of 1

Show 10 records per page

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATION PROTOCOL	MEDIA REALM
0	S4B	DefaultSRD	LAN_IF	SBC	0	0	5067	No encapsulation	--
1	ITSP	DefaultSRD	WAN_IF	SBC	5060	0	0	No encapsulation	--



Note: Current software releases uses the string **names** of the configuration entities (e.g., SIP Interface, Proxy Sets, and IP Groups). Therefore, it is recommended to configure each configuration entity with meaningful names for easy identification.

4.5 Step 5: Configure Proxy Sets

This step 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.

In the example scenario, two Proxy Sets need to be configured for the following IP entities:

- Mediant CCE
- ITSP SIP Trunk

The Proxy Sets will be later 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. Add a Proxy Set for the Mediant CCE as shown below:

Parameter	Value
Index	1
Name	S4B
SBC IPv4 SIP Interface	S4B
Proxy Keep-Alive	Using Options
Proxy Hot Swap	Enable
Load Balancing Method	Round Robin

Figure 4-9: Configuring Proxy Set for CCE

The screenshot shows the 'Proxy Sets [S4B]' configuration window. At the top, there is a dropdown for 'SRD' set to '#0 [DefaultSRD]'. Below this are four main sections: 'GENERAL', 'REDUNDANCY', 'KEEP ALIVE', and 'ADVANCED'. The 'GENERAL' section includes fields for Index (1), Name (S4B), Gateway IPv4 SIP Interface (--), SBC IPv4 SIP Interface (#0 [S4B]), and TLS Context Name (--). The 'REDUNDANCY' section includes Redundancy Mode (Homing), Proxy Hot Swap (Enable), Proxy Load Balancing Method (Round Robin), and Min. Active Servers for Load Balancing (1). The 'KEEP ALIVE' section includes Proxy Keep-Alive (Using OPTIONS), Proxy Keep-Alive Time [sec] (60), and Keep-Alive Failure Responses. The 'ADVANCED' section includes Classification Input (IP Address only) and DNS Resolve Method. At the bottom, there are 'Cancel' and 'APPLY' buttons.

- a. Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
- b. Click **New**
- c. Configure the address of the Proxy Set according to the parameters described in the table below.

Parameter	Value
Index	0
Proxy Address	10.15.70.83:5067 (Primary CCE IP address / FQDN and destination port)
Transport Type	TLS

- d. If there is additional CCE on the Site, Configure the parameters as described in the table below:

Parameter	Value
Index	1
Proxy Address	10.15.70.93:5067 (Secondary CCE IP address / FQDN and destination port)
Transport Type	TLS

- e. Click **Apply**.

3. Configure a Proxy Set for the ITSP SIP Trunk:

Parameter	Value
Index	2
Name	ITSP
SBC IPv4 SIP Interface	ITSP
Proxy Keep-Alive	Using Options
Keep-Alive Failure responses	503 (If this is received in response to a keep-alive message using SIP OPTIONS, the SBC considers the proxy as down and tries the next proxy.)
Proxy Hot Swap	Enable

Figure 4-10: Configuring Proxy Set for ITSP SIP Trunk

- a. Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
- b. Click **New**; the following dialog box appears:

Figure 4-11: Configuring Proxy Address for ITSP SIP Trunk

- c. Configure the address of the Proxy Set according to the parameters described in the table below.

Parameter	Value
Index	0
Proxy Address	ITSP.com:5060 (IP address / FQDN and destination port)
Transport Type	UDP

- d. Click **Apply**.

4.6 Step 6: Configure Coders

This step describes how to configure coders (termed *Coder Group*). As Skype for Business CCE supports the G.711 coder while the network connection to ITSP SIP Trunk may restrict operation with a lower bandwidth coder such as G.729, you need to add a Coder Group with the G.729 coder for the ITSP SIP Trunk.

Note that the Coder Group ID for this entity will be assign 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 CCE:

Parameter	Value
Coder Group ID	1
Coder Name	<ul style="list-style-type: none"> ▪ G.711 U-law ▪ G.711 A-law
Silence Suppression	Enable (for both coders)

Figure 4-12: Configuring Coder Group for CCE

Coder Groups

Coder Group Name 1 : AudioCodersGroups_1

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	Coder Specific
G.711U-law	20	64	0	Enable	
G.711A-law	20	64	8	Enable	

3. Configure a Coder Group for ITSP SIP Trunk:

Parameter	Value
Coder Group ID	2
Coder Name	G.729

Figure 4-13: Configuring Coder Group for ITSP SIP Trunk

Coder Groups

Coder Group Name 2 : AudioCodersGroups_2

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	Coder Specific
G.729	20	8	18	Disabled	

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the ITSP SIP Trunk uses the G.729 coder whenever possible. Note that this Allowed Coders Group ID will be assigned to the IP Profile belonging to the ITSP SIP Trunk Profile in the next step.

➤ **To set a preferred coder for the ITSP SIP Trunk:**

1. Open the Allowed Audio Coders Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Allowed Audio Coders Groups**).
2. Click **New** and configure a name for the Allowed Audio Coders Group for ITSP SIP Trunk.

Figure 4-14: Configuring Allowed Coders Group for ITSP SIP Trunk

Allowed Audio Coders Groups [ITSP Allowed Coders]

GENERAL

Index: 2

Name: • ITSP Allowed Coders

3. Click **Apply**.
4. Select the new row that you configured, and then click the **Allowed Audio Coders** link located below the table; the Allowed Audio Coders table opens.
5. Click **New** and configure an Allowed Coders as follows:

Parameter	Value
Index	0
Coder	G.729

Figure 4-15: Configuring Allowed Coders for ITSP SIP Trunk

Allowed Audio Coders

GENERAL

Index: 0

Coder: • G.729

User-defined Coder:

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

Figure 4-16: SBC Preferences Mode

Media Settings

GENERAL		ROBUSTNESS	
NAT Traversal	Disable NAT	New RTP Stream Packets	3
Enable Continuity Tones	Disable	New RTCP Stream Packets	3
Inbound Media Latch Mode	Dynamic	New SRTP Stream Packets	3
Number of Media Channels	0	New SRTCP Stream Packets	3
Enforce Media Order	Disable	Timeout To Relatch RTP (msec)	200
SDP Session Owner	AudiocodesGW	Timeout To Relatch SRTP (msec)	200
		Timeout To Relatch Silence (msec)	10000
		Timeout To Relatch RTCP (msec)	10000

SBC SETTINGS

Preferences Mode	• Include Extensions
Enforce Media Order	Disable

GATEWAY SETTINGS

Enable Early Media	Disable
Multiple Packetization Time Format	None

Cancel
APPLY

7. From the '**Preferences Mode**' drop-down list, select **Include Extensions**.
8. Click **Apply**.

4.7 Step 7: Configure IP Profiles

This step 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).

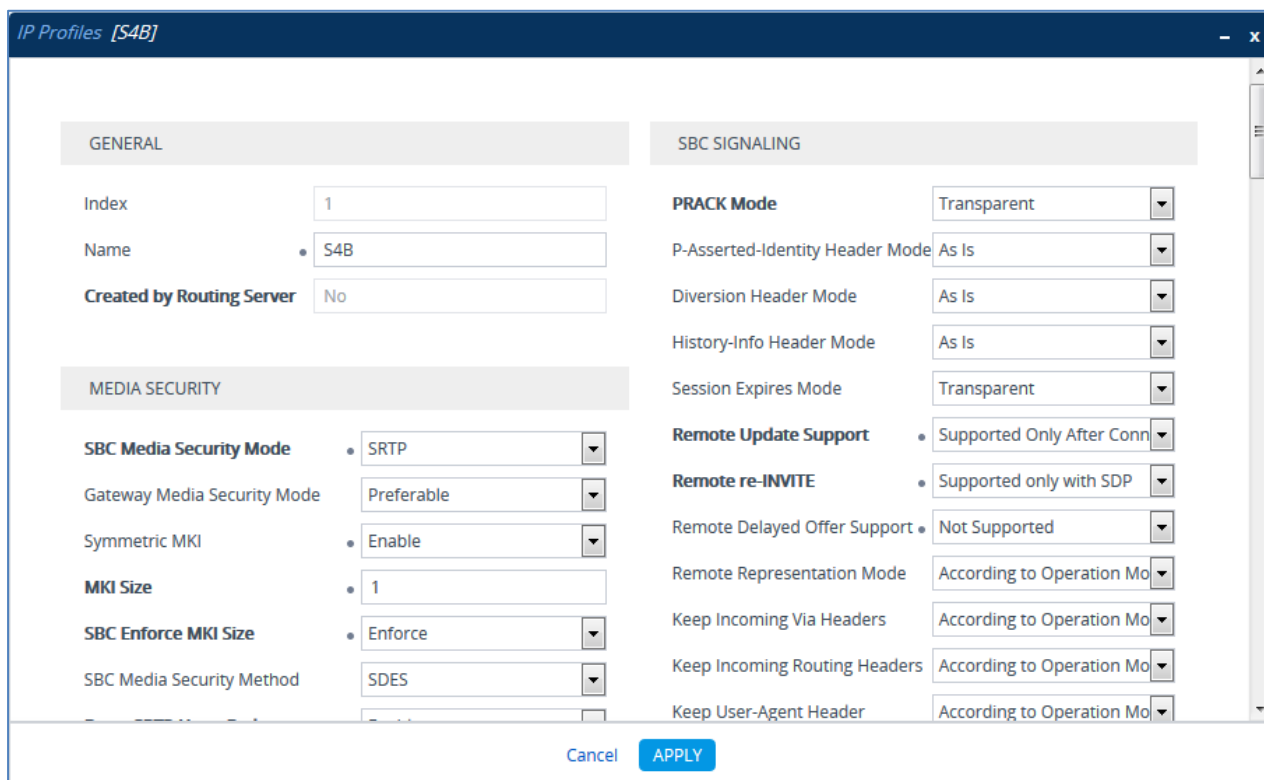
In the example scenario, IP Profiles need to be configured for the following IP entities:

- Microsoft Skype for Business CCE - to operate in secure mode using SRTP and TLS
- ITSP SIP trunk - to operate in non-secure mode using RTP and UDP

➤ **To configure IP Profile for the CCE:**

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	S4B
Media Security	
SBC Media Security Mode	SRTP
Symmetric MKI	Enable
MKI Size	1
Enforce MKI Size	Enforce
Reset SRTP State Upon Re-key	Enable
Generate SRTP Keys Mode:	Always
SBC Early Media	
Remote Early Media RTP Detection Mode	By Media (required, as Skype for Business CCE does not send RTP immediately to remote side when it sends a SIP 18x response)
SBC Media	
Extension Coders Group	AudioCodersGroups_1
SBC Signaling	
Remote Update Support	Supported Only After Connect
Remote re-INVITE Support	Supported Only With SDP
Remote Delayed Offer Support	Not Supported
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally (required, as CCE does not support receipt of SIP REFER)
Remote 3xx Mode	Handle Locally (required, as CCE does not support receipt of SIP 3xx responses)

Figure 4-17: Configuring IP Profile for CCE


IP Profiles [S4B]

GENERAL	SBC SIGNALING
Index: 1	PRACK Mode : Transparent
Name: S4B	P-Asserted-Identity Header Mode: As Is
Created by Routing Server: No	Diversion Header Mode: As Is
	History-Info Header Mode: As Is
	Session Expires Mode: Transparent
	Remote Update Support : Supported Only After Conn
	Remote re-INVITE : Supported only with SDP
	Remote Delayed Offer Support: Not Supported
	Remote Representation Mode: According to Operation Mo
	Keep Incoming Via Headers: According to Operation Mo
	Keep Incoming Routing Headers: According to Operation Mo
	Keep User-Agent Header: According to Operation Mo

Buttons: Cancel, APPLY

3. Click Apply.

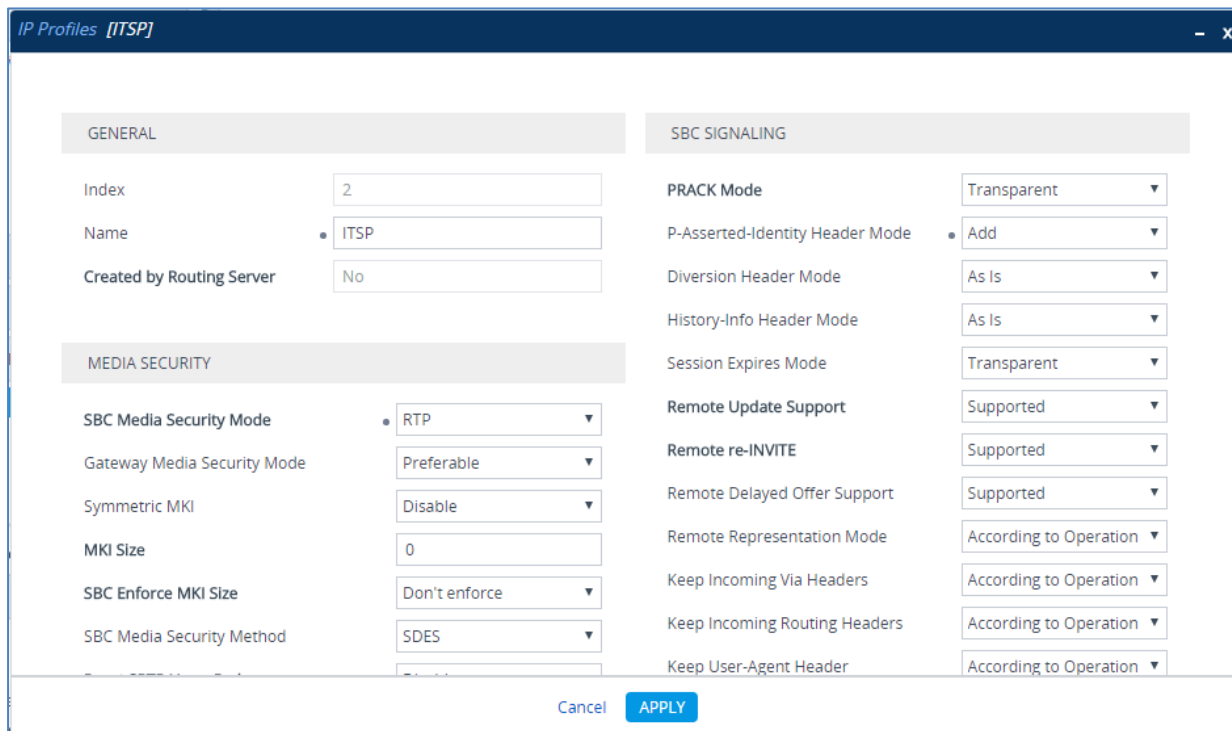
➤ **To configure an IP Profile for the ITSP SIP Trunk:**

1. Click **New**, and then configure the parameters as follows:

Parameter	Value
General	
Index	2
Name	ITSP
Media Security	
SBC Media Security Mode	RTP
SBC Early Media	
Remote Can Play Ringback	No (required, as CCE does not provide a ringback tone for incoming calls)
SBC Media	
Extension Coders Group	AudioCodersGroups_2
Allowed Audio Coders	ITSP Allowed Coders
Allowed Coders Mode	Preference (lists Allowed Coders first and then original coders in received SDP offer)
SBC Signaling	
P-Asserted-Identity Header Mode	Add (required for anonymous calls)



Note: The SIP Trunk's IP Profile depends on the SIP Trunk behavior. Refer to the explanations of the IP Profile parameters in the *SBC User's Manual* in order to configure the profile according to SIP Trunk behavior.

Figure 4-18: Configuring IP Profile for ITSP SIP Trunk


IP Profiles [ITSP]

GENERAL		SBC SIGNALING	
Index	2	PRACK Mode	Transparent
Name	ITSP	P-Asserted-Identity Header Mode	Add
Created by Routing Server	No	Diversion Header Mode	As Is
		History-Info Header Mode	As Is
		Session Expires Mode	Transparent
		Remote Update Support	Supported
		Remote re-INVITE	Supported
		Remote Delayed Offer Support	Supported
		Remote Representation Mode	According to Operation
		Keep Incoming Via Headers	According to Operation
		Keep Incoming Routing Headers	According to Operation
		Keep User-Agent Header	According to Operation

Cancel **APPLY**

2. Click Apply.

4.8 Step 8: Configure IP Groups

This step describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the E-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 the example scenario, IP Groups must be configured for the following IP entities:

- CCE (Mediation Server) located on LAN
- ITSP SIP Trunk located on WAN

➤ **To configure IP Groups:**

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

Parameter	Value
Index	1
Name	S4B
Type	Server
Proxy Set	S4B
IP Profile	S4B
Media Realm	MRLan
SIP Group Name	(according to ITSP requirement)

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

Parameter	Value
Index	2
Name	ITSP
Topology Location	Up
Type	Server
Proxy Set	ITSP
IP Profile	ITSP
Media Realm	MRWan
SIP Group Name	(according to ITSP requirement)

The configured IP Groups are shown in the figure below:

Figure 4-19: Configured IP Groups in IP Group Table

IP Groups (3)

+ 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 MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
0	Default_IPG	DefaultS	Server	Not Configur	ProxySet_0	--	--		Disable	-1	-1
1	S4B	DefaultS	Server	Not Configur	S4B	S4B	MRLan		Enable	-1	-1
2	ITSP	DefaultS	Server	Not Configur	ITSP	ITSP	MRWan		Enable	-1	-1

4.9 Step 9: SIP TLS Connection Configuration

This section describes how to configure the E-SBC for using a TLS connection with the CCE Mediation Server. This is essential for a secure SIP TLS connection.

4.9.1 Step 9a: 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 E-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., **10.15.27.1**).

Figure 4-20: Configuring NTP Server Address

NTP SERVER	
Primary NTP Server Address (IP or FQDN)	• 10.15.27.1
Secondary NTP Server Address (IP or FQDN)	
NTP Update Interval	Hours: 24 Minutes: 0
NTP Authentication Key Identifier	0
NTP Authentication Secret Key	

3. Click **Apply**.

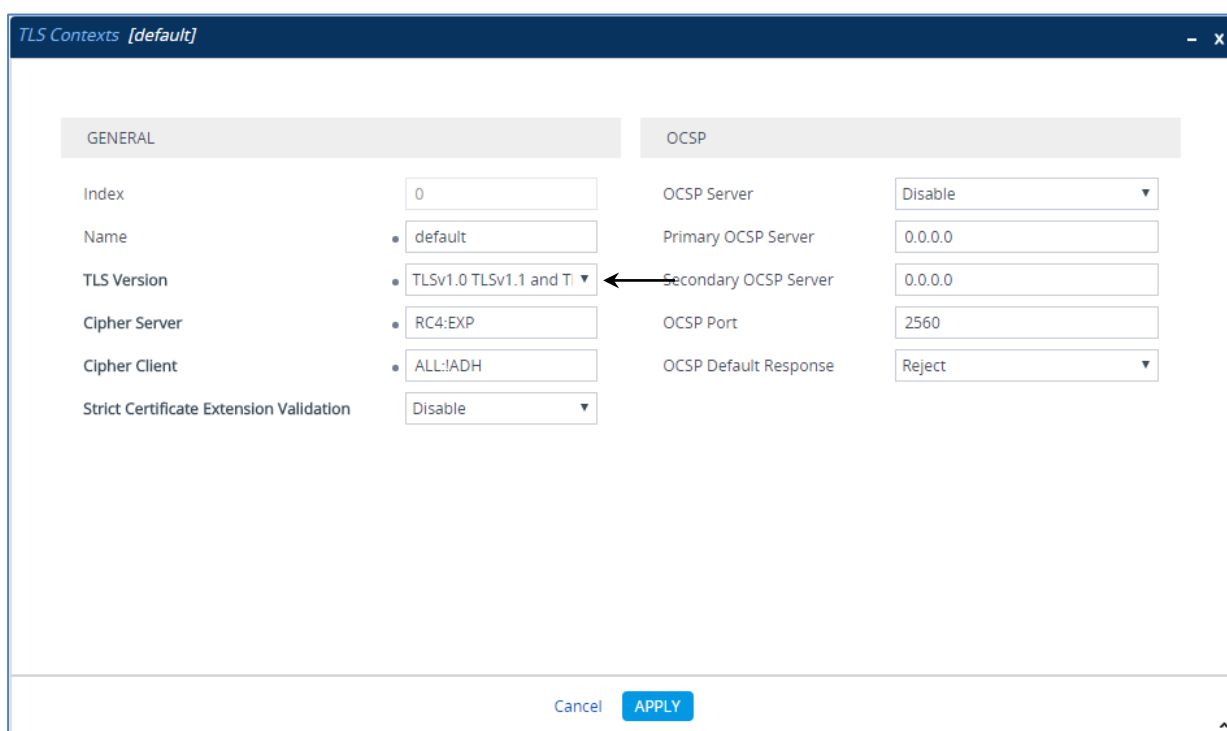
4.9.2 Step 9b: Configure the TLS version

This step describes how to configure the E-SBC to use TLS 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 **'TLSv1.0 TLSv1.1 and TLSv1.2'**

Figure 4-21: Configuring TLS version



The screenshot shows the 'TLS Contexts [default]' configuration window. It has two tabs: 'GENERAL' and 'OCSP'. The 'GENERAL' tab is active, showing the following fields:

- Index:** 0
- Name:** default
- TLS Version:** TLSv1.0 TLSv1.1 and TLSv1.2 (selected)
- Cipher Server:** RC4:EXP
- Cipher Client:** ALL:!ADH
- Strict Certificate Extension Validation:** Disable

The 'OCSP' tab is also visible, showing the following fields:

- OCSP Server:** Disable
- Primary OCSP Server:** 0.0.0.0
- Secondary OCSP Server:** 0.0.0.0
- OCSP Port:** 2560
- OCSP Default Response:** Reject

At the bottom of the window, there are 'Cancel' and 'APPLY' buttons. An arrow points to the 'TLS Version' dropdown in the 'GENERAL' tab.

4. Click **Apply**.

4.9.3 Step 9c: Configure a Certificate

This step describes how to exchange a certificate with Microsoft Certificate Authority (CA) inside the DC. The certificate is used by the E-SBC to authenticate the connection with Mediant CCE.



Note: The CCE Wizard supports applying Certificates to the SBC (refer to *LTRT-28086 Mediant Appliance for Microsoft Skype for Business CCE Installation Manual Ver. 2.0.2* Section “Set the GW/SBC Certificate”).

- Reset the E-SBC with a burn to flash for your settings to take effect (see Section [4.17](#) on page [54](#)).

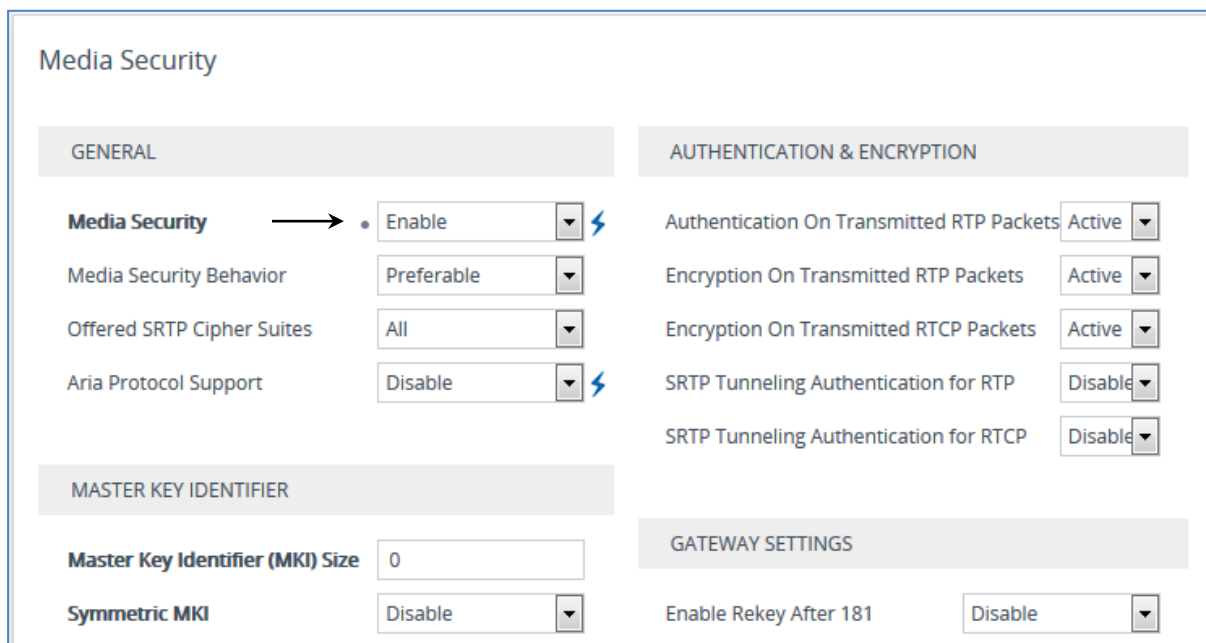
4.10 Step 10: Configure SRTP

This step describes how to configure media security. If you configure the Mediation Server to use SRTP, you need to configure the E-SBC to operate in the same manner. Note that SRTP was enabled for the CCE when you configured an IP Profile for Skype for Business CCE (see Section 4.6 on page 28).

➤ **To configure media security:**


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

Figure 4-22: Configuring SRTP




Media Security

GENERAL

Media Security → • Enable 

Media Security Behavior: Preferable

Offered SRTP Cipher Suites: All

Aria Protocol Support: Disable 

AUTHENTICATION & ENCRYPTION

Authentication On Transmitted RTP Packets: Active

Encryption On Transmitted RTP Packets: Active

Encryption On Transmitted RTCP Packets: Active

SRTP Tunneling Authentication for RTP: Disable

SRTP Tunneling Authentication for RTCP: Disable

MASTER KEY IDENTIFIER

Master Key Identifier (MKI) Size: 0

Symmetric MKI: Disable

GATEWAY SETTINGS

Enable Rekey After 181: Disable

2. From the 'Media Security' drop-down list, select **Enable** to enable SRTP.
3. Click **Apply**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.17 on page 54).

4.11 Step 11: Configure Maximum IP Media Channels

This step describes how to configure the maximum number of required IP media channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to call sessions.



Note: This step is mandatory **only** if transcoding is required.

➤ **To configure the maximum number of IP media channels:**

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

Figure 4-23: Configuring Number of Media Channels

2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., 100).
3. Click **Apply**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.17 on page 54).

4.12 Step 12: Configure IP-to-IP Call Routing Rules

This step 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 E-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. The routing rules use the configured IP Groups (as configured in Section 4.8 on page 35,) to denote the source and destination of the call.

In the example scenario, the following IP-to-IP routing rules need to be configured to route calls between Skype for Business CCE (LAN) and ITSP SIP Trunk (DMZ):

- Terminate SIP OPTIONS messages on the E-SBC that are received from the both LAN and DMZ
- Calls from CCE to ITSP SIP Trunk
- Calls from ITSP SIP Trunk to CCE

➤ 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 a rule to terminate SIP OPTIONS messages received from the both LAN and DMZ:
 - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	0
Name	Terminate OPTIONS (arbitrary descriptive name)
Source IP Group	Any
Request Type	OPTIONS
Destination Type	Dest Address
Destination Address	internal

Figure 4-24: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS

IP-to-IP Routing [Terminate OPTIONS]

Routing Policy #0 [Default_SBCRoutingPolicy]

GENERAL

Index 0

Name • Terminate OPTIONS

Alternative Route Options Route Row

MATCH

Source IP Group Any View

Request Type • OPTIONS

Source Username Prefix *

Source Host *

Source Tags

ACTION

Destination Type • Dest Address

Destination IP Group -- View

Destination SIP Interface -- View

Destination Address • internal

Destination Port 0

Destination Transport Type

Call Setup Rules Set ID -1

Group Policy Sequential

Cost Group -- View

Cancel APPLY

- b. Click **Apply**.
3. Configure a rule to route calls from CCE to ITSP SIP Trunk:
 - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	1
Name	S4B to ITSP (arbitrary descriptive name)
Source IP Group	S4B
Destination Type	IP Group
Destination IP Group	ITSP
Destination SIP Interface	ITSP

Figure 4-25: Configuring IP-to-IP Routing Rule for S4B to ITSP

IP-to-IP Routing [S4B to ITSP]

Routing Policy #0 [Default_SBCRoutingPolicy]

GENERAL

Index 1

Name S4B to ITSP

Alternative Route Options Route Row

MATCH

Source IP Group #1 [S4B] View

Request Type All

Source Username Prefix *

Source Host *

Source Tag

ACTION

Destination Type IP Group

Destination IP Group #2 [ITSP] View

Destination SIP Interface #1 [ITSP] View

Destination Address

Destination Port 0

Destination Transport Type

Call Setup Rules Set ID -1

Group Policy Sequential

Cost Group -- View

Cancel APPLY

- b.** Click **Apply**.

4. Configure rule to route calls from ITSP SIP Trunk to CCE:
 - a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	2
Name	ITSP to S4B (arbitrary descriptive name)
Source IP Group	ITSP
Destination Type	IP Group
Destination IP Group	S4B
Destination SIP Interface	S4B

Figure 4-26: Configuring IP-to-IP Routing Rule for ITSP to S4B

The screenshot shows the 'IP-to-IP Routing [ITSP to S4B]' configuration window. At the top, the 'Routing Policy' is set to '#0 [Default_SBCRoutingPolicy]'. The window is divided into three main sections: GENERAL, MATCH, and ACTION.

GENERAL Section:

- Index: 2
- Name: ITSP to S4B
- Alternative Route Options: Route Row

MATCH Section:

- Source IP Group: #2 [ITSP] (with a 'View' link)
- Request Type: All
- Source Username Prefix: *
- Source Host: *
- Source Tag: (empty)

ACTION Section:

- Destination Type: IP Group
- Destination IP Group: #1 [S4B] (with a 'View' link)
- Destination SIP Interface: #0 [S4B] (with a 'View' link)
- Destination Address: (empty)
- Destination Port: 0
- Destination Transport Type: (empty)
- Call Setup Rules Set ID: -1
- Group Policy: Sequential
- Cost Group: -- (with a 'View' link)

At the bottom of the window, there are 'Cancel' and 'APPLY' buttons.

- b. Click **Apply**.

The configured routing rules are shown in the figure below:

Figure 4-27: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

IP-to-IP Routing (3)

+ New Edit Insert

↑ ↓

🗑️

⏪ <<

Page 1 of 1

>> ⏩

Show 10 records per page

INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PREFIX	DESTINATION USERNAME PREFIX	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	Terminate O	Default_SBC	Route Row	Any	OPTIONS	*	*	Dest Address	--	--	internal
1	S4B to ITSP	Default_SBC	Route Row	S4B	All	*	*	IP Group	ITSP	ITSP	
2	ITSP to S4B	Default_SBC	Route Row	ITSP	All	*	*	IP Group	S4B	S4B	



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

4.13 Step 13: Configure IP-to-IP Manipulation Rules

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Section 4.8 on page 35) to denote the source and destination of the call.



Note: Adapt the manipulation table according to your environment dial plan.

For this example scenario, a manipulation is configured to add the "+" (plus sign) to the destination number for calls from the ITSP SIP Trunk IP Group to the CCE IP Group for any destination username prefix.

➤ **To configure a number manipulation rule:**

1. Open the Outbound Manipulations table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Manipulation** > **Outbound Manipulations**).
2. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	0
Name	Add + toward S4B
Source IP Group	SP
Destination IP Group	S4B
Destination Username Prefix	* (asterisk sign)
Manipulated Item	Destination URI
Prefix to Add	+ (plus sign)

Figure 4-28: Configuring IP-to-IP Outbound Manipulation Rule

Outbound Manipulations [Add + toward S4B]

Routing Policy #0 [Default_SBCRoutingPolicy]

GENERAL

Index 0

Name Add + toward S4B

Additional Manipulation No

Call Trigger Any

MATCH

Request Type All

Source IP Group #2 [ITSP] View

Destination IP Group #1 [S4B] View

Source Username Prefix *

ACTION

Manipulated Item Destination URI

Remove From Left 0

Remove From Right 0

Leave From Right 255

Prefix to Add +

Suffix to Add

Privacy Restriction Mode Transparent

Cancel APPLY

3. Click **Apply**.

The figure below shows an example of configured IP-to-IP outbound manipulation rules for calls between CCE IP Group and ITSP SIP Trunk IP Group:

Figure 4-29: Example of Configured IP-to-IP Outbound Manipulation Rules

Outbound Manipulations (3)

+ New Edit Insert

Page 1 of 1 Show 10 records per page

INDEX	NAME	ROUTING POLICY	ADDITIONAL MANIPULATION	SOURCE IP GROUP	DESTINATION IP GROUP	SOURCE USERNAME PREFIX	DESTINATION USERNAME PREFIX	MANIPULATED ITEM	REMOVE FROM LEFT	REMOVE FROM RIGHT	LEAVE FROM RIGHT	PREFIX TO ADD	SUFFIX TO ADD
0	Add + toward	Default_SE	No	ITSP	S4B	*	*	Destination	0	0	255	+	
1	Remove +	Default_SE	No	S4B	ITSP	*	+	Destination	1	0	255		
2	Remove +	Default_SE	No	S4B	ITSP	+	*	Source UR	1	0	255		

Rule Index	Description
1	Calls from ITSP IP Group to S4B IP Group with any destination number (*), add "+" to the prefix of the destination number.
2	Calls from S4B IP Group to ITSP IP Group with the prefix destination number "+", remove "+" from this prefix.
3	Calls from S4B IP Group to ITSP IP Group with source number prefix "+", remove the "+" from this prefix.

4.14 Step 14: Configure Message Manipulation Rules

This step 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.

See an example below of a message manipulation rule configuration; use the *SBC User's Manual* for detailed instructions on how to configure message manipulation rules according to your requirements.

In the example scenario, the configured manipulation rule replaces the user part of the SIP From Header with the value from the SIP History-Info Header.

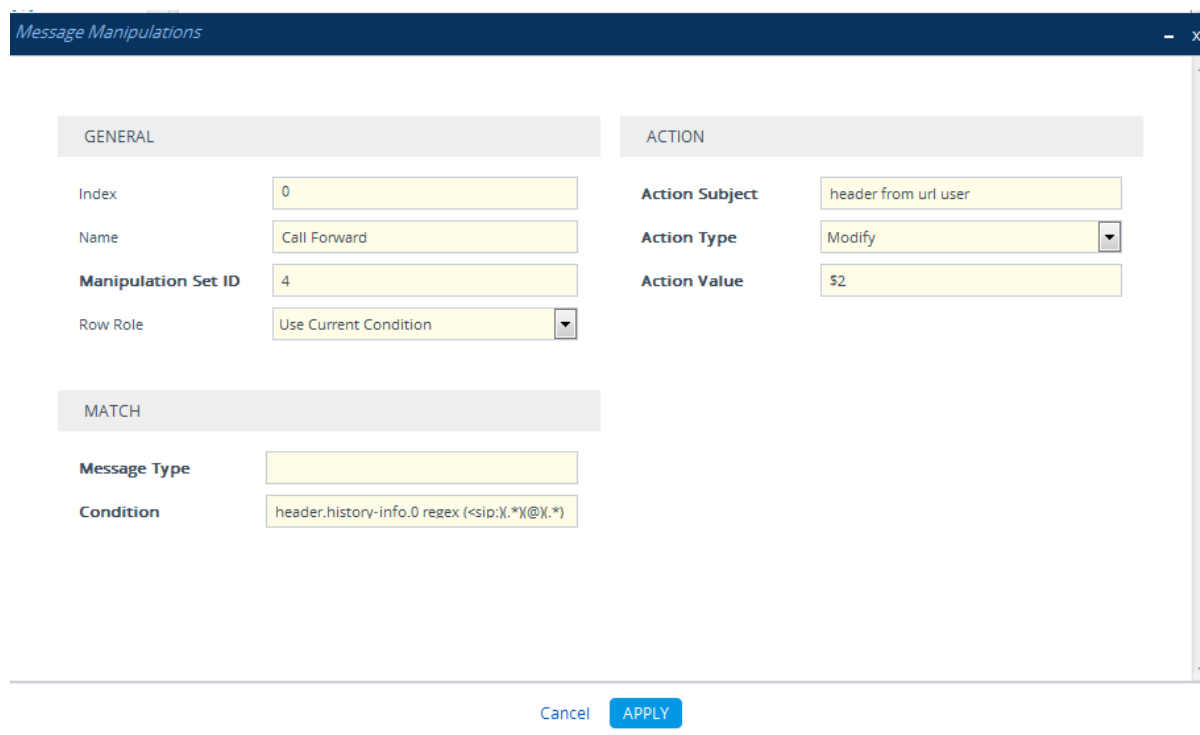


Note: The History-info header isn't set by default, in order to use the below MMS need to enable *ForwardCallHistory* parameter on the CCE Trunk Configuration.

➤ 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 new manipulation rule (Manipulation Set 4) for ITSP SIP Trunk. This rule applies to messages sent to the ITSP SIP Trunk IP Group in a call forward scenario.

Parameter	Value
Index	0
Name	Call Forward
Manipulation Set ID	4
Message Type	invite.request
Condition	header.history-info.0 regex (<sip:)(.*)(@)(.*)
Action Subject	header.from.url.user
Action Type	Modify
Action Value	\$2

Figure 4-30: Configuring SIP Message Manipulation Rule 0 (for ITSP SIP Trunk)


Message Manipulations

GENERAL

Index: 0

Name: Call Forward

Manipulation Set ID: 4

Row Role: Use Current Condition

ACTION

Action Subject: header from url user

Action Type: Modify

Action Value: \$2

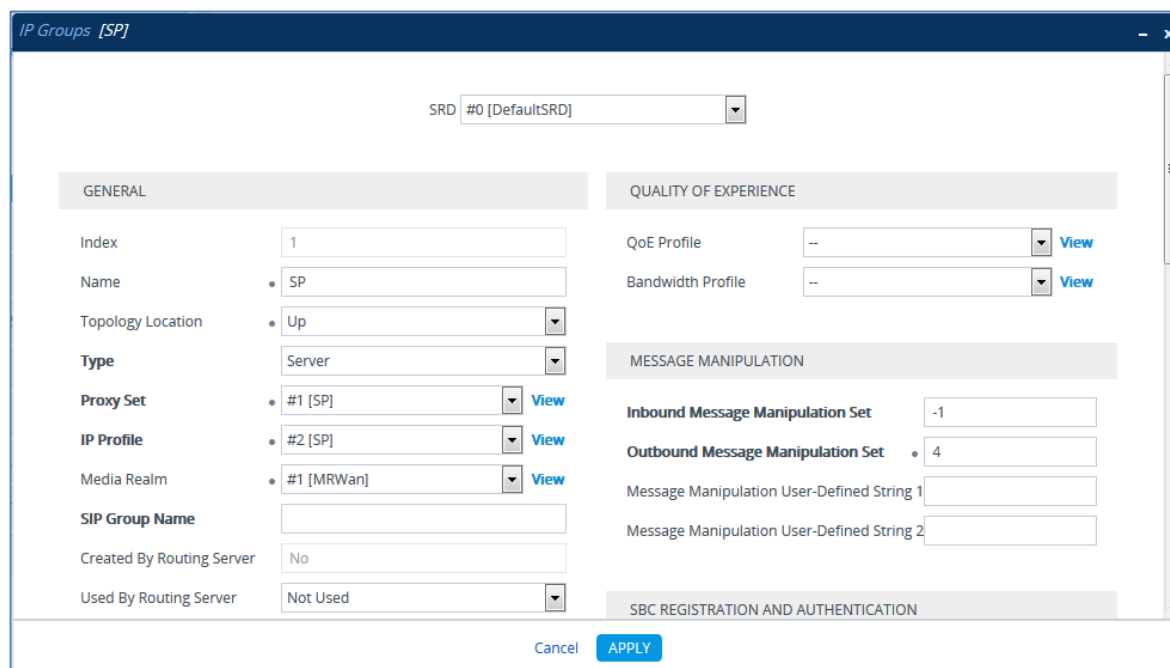
MATCH

Message Type:

Condition: header.history-info.0 regex (< sip: X. *) (@) X. *)

Cancel APPLY

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

Figure 4-31: Assigning Manipulation Set 4 to the ITSP SIP Trunk IP Group


IP Groups [SP]

SRD: #0 [DefaultSRD]

GENERAL

Index: 1

Name: SP

Topology Location: Up

Type: Server

Proxy Set: #1 [SP]

IP Profile: #2 [SP]

Media Realm: #1 [MRWan]

SIP Group Name:

Created By Routing Server: No

Used By Routing Server: Not Used

QUALITY OF EXPERIENCE

QoE Profile: --

Bandwidth Profile: --

MESSAGE MANIPULATION

Inbound Message Manipulation Set: -1

Outbound Message Manipulation Set: 4

Message Manipulation User-Defined String 1:

Message Manipulation User-Defined String 2:

Cancel APPLY

- d. Click **Apply**.

4.15 Step 15: Configure Registration Accounts

This step describes how to configure SIP registration accounts. This is required so that the E-SBC can register with the ITSP SIP Trunk on behalf of CCE. The ITSP SIP Trunk requires registration and authentication to provide service.

In the interoperability test topology, the Served IP Group is CCE IP Group and the Serving IP Group is ITSP SIP Trunk IP Group.

➤ **To configure a registration account:**

1. Open the Accounts table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Accounts**).
2. Click **New**.
3. Configure the account according to the provided information from , for example:

Parameter	Value
Served IP Group	S4B
Application Type	SBC
Serving IP Group	ITSP
Host Name	As provided by the SIP Trunk provider
Register	Regular
Contact User	1234567890 (trunk main line)
User Name	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

Figure 4-32: Configuring a SIP Registration Account

The screenshot shows the 'Accounts' configuration window. At the top, there is a dropdown for 'Served IP Group' with the value '#1 [S4B]'. Below this, the window is divided into two main sections: 'GENERAL' and 'CREDENTIALS'.

GENERAL Section:

- Index: 0
- Served Trunk Group: -1
- Application Type: SBC (selected from a dropdown)
- Serving IP Group: #2 [ITSP] (selected from a dropdown, with a 'View' link next to it)
- Host Name: HostName.com
- Register: Regular (selected from a dropdown)
- Contact User: 1234567890

CREDENTIALS Section:

- User Name: UserName
- Password: *

At the bottom of the window, there are two buttons: 'Cancel' and 'APPLY'.

4. Click **Apply**.

4.16 Step 16: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

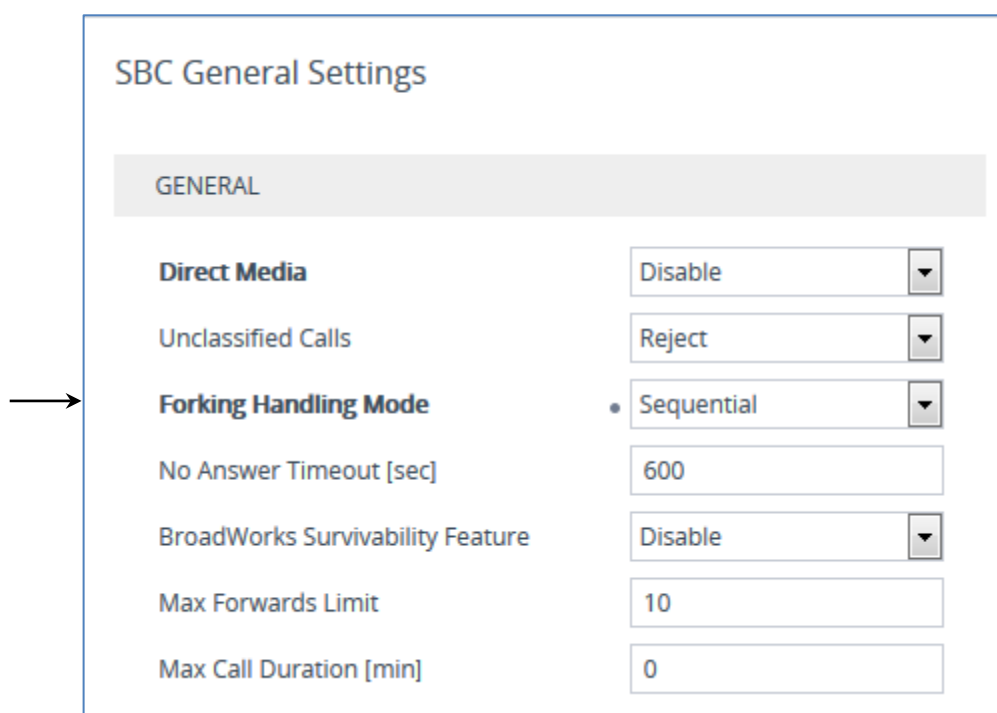
4.16.1 Step 16a: Configure Call Forking Mode

This step describes how to configure the E-SBC's handling of SIP 18x responses received for call forking of INVITE messages. In the example scenario, if a SIP 18x response with SDP is received, the E-SBC opens a voice stream according to the received SDP. The E-SBC re-opens the stream according to subsequently received 18x responses with SDP or plays a ringback tone if a 180 response without SDP is received. It is mandatory to set this field for the Skype for Business CCE environment.

➤ **To configure call forking:**

1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).
2. From the 'SBC Forking Handling Mode' drop-down list, select **Sequential**.

Figure 4-33: Configuring Forking Mode



The screenshot shows the 'SBC General Settings' page. A horizontal arrow points to the 'Forking Handling Mode' dropdown menu, which is currently set to 'Sequential'. The page includes several other settings:

GENERAL	
Direct Media	Disable
Unclassified Calls	Reject
Forking Handling Mode	Sequential
No Answer Timeout [sec]	600
BroadWorks Survivability Feature	Disable
Max Forwards Limit	10
Max Call Duration [min]	0

3. Click **Apply**.

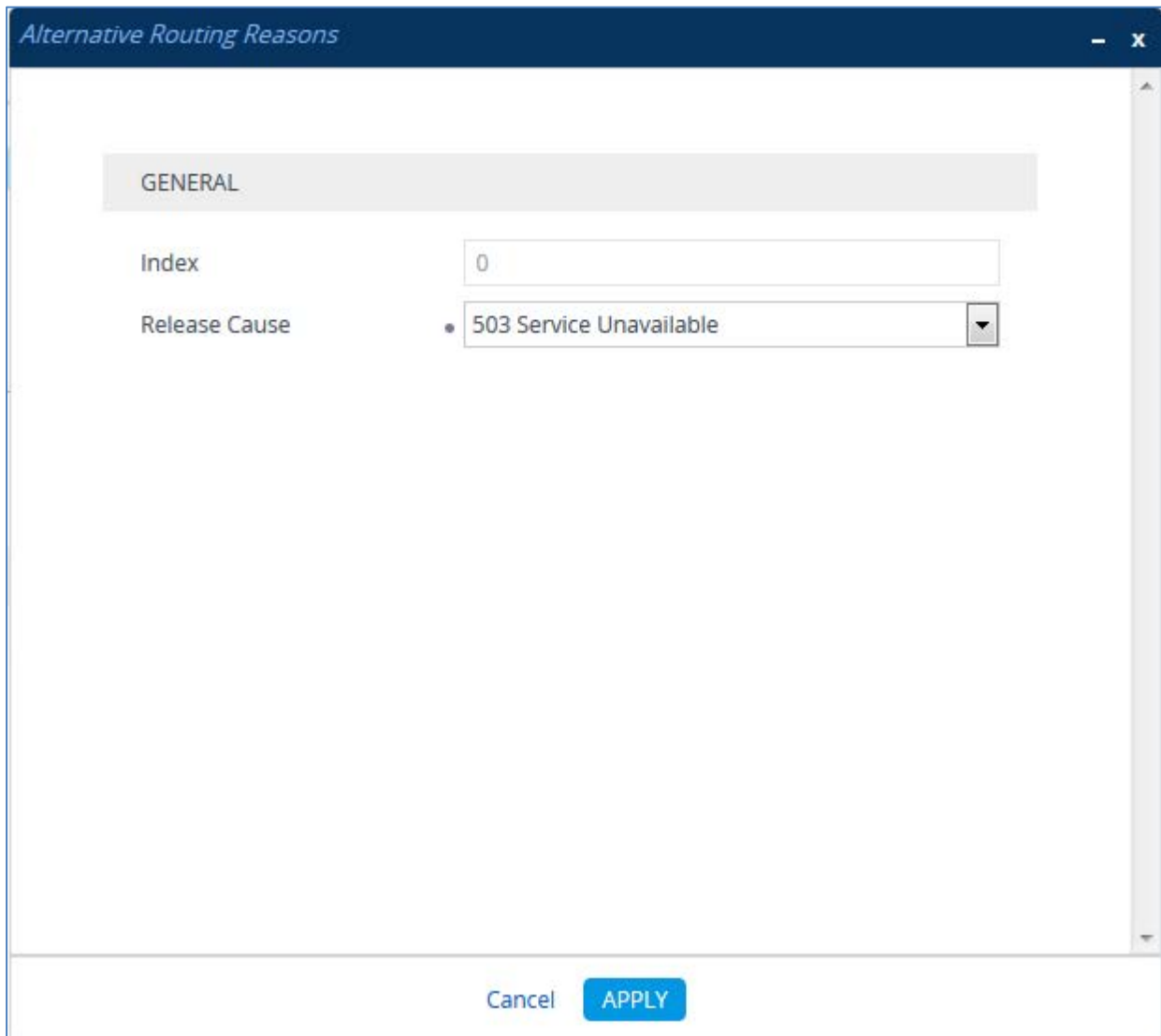
4.16.2 Step 16b: Configure SBC Alternative Routing Reasons

This step describes how to configure the E-SBC's handling of SIP 503 responses received for outgoing SIP dialog-initiating methods, e.g., INVITE, OPTIONS, and SUBSCRIBE messages. In this case E-SBC attempts to locate an alternative route for the call.

➤ To configure SIP reason codes for alternative IP routing:

1. Open the Alternative Routing Reasons table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **Alternative Reasons**).
2. Click **New**.
3. From the 'Release Cause' drop-down list, select **503 Service Unavailable**.

Figure 4-34: SBC Alternative Routing Reasons Table



The screenshot shows a configuration window titled "Alternative Routing Reasons". It features a "GENERAL" tab. Under this tab, there are two configuration fields: "Index" with a text input field containing the value "0", and "Release Cause" with a dropdown menu currently displaying "503 Service Unavailable". At the bottom of the window, there are two buttons: "Cancel" and "APPLY".

4. Click **Apply**.

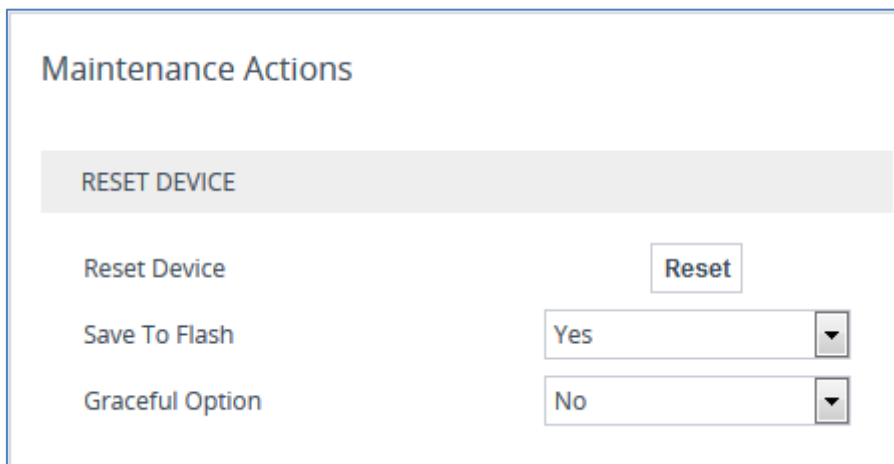
4.17 Step 17: Reset the E-SBC

After you have completed the configuration of the E-SBC described in this chapter, save ("burn") the configuration to the E-SBC's flash memory with a reset for the settings to take effect.

➤ **To reset the device through Web interface:**

1. Open the Maintenance Actions page (**Setup** menu > **Administration** tab > **Maintenance** folder > **Maintenance Actions**).

Figure 4-35: Resetting the E-SBC



The screenshot shows the 'Maintenance Actions' web page. At the top, there is a section titled 'RESET DEVICE' in a light gray box. Below this, there are three rows of controls:

RESET DEVICE	
Reset Device	<input type="button" value="Reset"/>
Save To Flash	<input type="text" value="Yes"/> ▼
Graceful Option	<input type="text" value="No"/> ▼

2. Ensure that the ' Save To Flash' field is set to **Yes** (default).
3. Click the **Reset** button; a confirmation message box appears, requesting you to confirm.
4. Click **OK** to confirm device reset.

This page is intentionally left blank.

International Headquarters

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

AudioCodes Inc.

27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: www.audiocodes.com/info

Website: www.audiocodes.com

©2017 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-28160

