Configuration Note

AudioCodes Professional Services – Interoperability Lab

Connecting Cisco Webex Calling with AudioCodes SBC

Table of Contents

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 can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: November-08-2022

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.

Related Documentation

Document Name
Mediant 500L Gateway and E-SBC User's Manual
Mediant 500 Gateway & E-SBC User's Manual
Mediant 800 Gateway & E-SBC User's Manual
Mediant 1000B Gateway & E-SBC User's Manual
Mediant 2600 E-SBC User's Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual
SIP Message Manipulation Reference Guide
AudioCodes Configuration Notes

Document Revision Record

LTRT	Description
12732	Initial document release.

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 website at https://online.audiocodes.com/documentation-feedback.

1 Introduction

This Configuration Note describes how to set up the AudioCodes Enterprise Session Border Controller (hereafter, referred to as *SBC*) for interworking between Audiocodes SIP Trunk and the Cisco Webex Calling environment.

You can also use AudioCodes' SBC Wizard tool to automatically configure the SBC based on this interoperability setup. However, it is recommended to read through this document to better understand the various configuration options. For more information on AudioCodes' SBC Wizard including the download option, visit AudioCodes website at https://www.audiocodes.com/partners/sbc-interoperability-list.

1.1 About Cisco Webex Calling

Webex Calling cloud service is Cisco's phone services from the cloud and the data sheet to this service is https://www.cisco.com/c/en/us/products/collateral/unified-communications/webexcalling/datasheet-c78-742056.html.

Webex Calling Cloud service or in short "Webex Calling" supports "Bring Your Own PSTN" and Enterprise dialing using through what is termed as a Local Gateway that sits at the edge of the Customer's VoIP network. A local gateway is a SIP Session Border Controller that works with Webex Calling Cloud service in specific ways. This local gateway MUST operate according to specific conditions with Webex Calling Cloud services.

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.

2 Component Information

2.1 AudioCodes SBC Version

Table 2-1: AudioCodes SBC Version

SBC Vendor	AudioCodes
Models	■ Mediant 500 Gateway & E-SBC ■ Mediant 800B/C Gateway & E-SBC ■ Mediant 1000B Gateway & E-SBC ■ Mediant 2600 E-SBC ■ Mediant 4000/B SBC ■ Mediant 9000, 9030, 9080 SBC ■ Mediant Software SBC (VE/SE/CE)
Software Version	7.40A.250.440 or later
Protocol	■ SIP/UDP or SIP/TCP or SIP/TLS (to the Audiocodes SIP Trunk) ■ SIP/TLS (to the Cisco Webex Calling system)
Additional Notes	None

2.2 Cisco Webex Calling System Version

Table 2-2: Cisco Webex Calling System Version

Vendor	Cisco
Model	BroadWorks
Software Version	
Protocol	SIP
Additional Notes	None

2.3 Audiocodes SIP Trunking Version

Table 2-3: Audiocodes Version

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

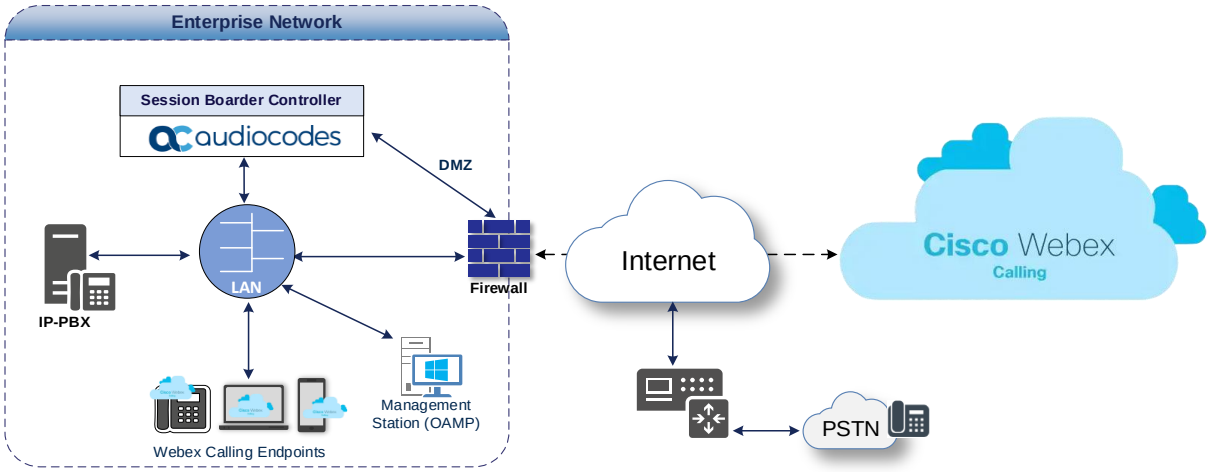
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes SBC and Audiocodes SIP Trunk with the Cisco Webex Calling system was done using the following topology setup:

- Enterprise deployed with the administrator's management station, Webex Calling endpoints and 3-rd party IP-PBX located on the LAN.
- Enterprise deployed with the Cisco Webex Calling system located on the WAN for enhanced communication within the Enterprise.
- Enterprise wishes to offer its employees enterprise-voice capabilities and to connect the Enterprise to the PSTN network using Audiocodes's SIP Trunking service.
- AudioCodes SBC implemented to interconnect between the SIP Trunk and the Cisco Webex Calling system.
  - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
  - **Border:** IP-to-IP network border - both, the Audiocodes's SIP Trunk and the Cisco Webex Calling system are located in the public network.

The figures below illustrate possible topologies:

Figure 2-1: Layout with SBC On-Prem Implementation



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	■ Both, Cisco Webex Calling system and Audiocodes SIP Trunk environments are located on the WAN.
Signaling Transcoding	■ Cisco Webex Calling system operates with SIP-over-TLS transport type. ■ Audiocodes SIP Trunk operates with SIP-over-UDP or SIP-over-TCP transport type.
Codecs Transcoding	■ Cisco Webex Calling system supports OPUS, G.711U-law and G.711A-law coders. ■ Audiocodes SIP Trunk supports G.711A-law, G.711U-law, and G.729 coders.
Media Transcoding	■ Cisco Webex Calling system operates with SRTP media type. ■ Audiocodes SIP Trunk operates with RTP media type.

2.4.2 Known Limitations

When ICE mode is enabled between the Cisco Webex Calling system and AudioCodes SBC, implementation of early media is different between Cisco and AudioCodes. That's why in this case, SBC will be configured with 'Remote Early Media = Not Supported' towards the Cisco Webex (refer to Section 4.8 on page 19). There were no other limitations observed in the interoperability tests performed for the AudioCodes SBC interworking between the Cisco Webex Calling system and Audiocodes's SIP Trunk.

3 Configuring Cisco Webex Calling

For configuring your Cisco Webex Calling setup, refer to the Webex Calling Configuration Workflow.

Before you begin configuration:

- Contact your local Cisco representative to enable Cisco Webex on your Corporate Cisco Webex account.
- Make sure you have Cisco Webex Control Hub Administrator credentials.

4 Configuring AudioCodes SBC

This section describes how to configure AudioCodes SBC for interworking between the Cisco Webex Calling system and the Audiocodes SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 3, and includes the following main areas:

- SBC LAN interface - Management Station
- SBC WAN interface - Audiocodes SIP Trunking and the Cisco Webex Calling system environment

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

- For implementing the Cisco Webex Calling system and Audiocodes SIP Trunk based on the configuration described in this section, AudioCodes SBC must be installed with a License Key that includes the following software features:
  - **Number of SBC sessions** [Based on requirements]
  - **DSP Channels** [If media transcoding is needed]
  - **Transcoding sessions** [If media transcoding is needed]
  - **Coders** [Based on requirements]

  For more information about the License Key, contact your AudioCodes sales representative.
- If your SBC is deployed in a virtual environment and transcoding is required, your virtual machine must have a minimum of 2 vCPUs. For more information, please refer to the appropriate *Installation Manual,* which can be found on AudioCodes website.
- 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 website

4.1 Prerequisites

Before you begin configuration, make sure you have obtained the following for each SBC you wish to pair with Cisco Webex Calling System:

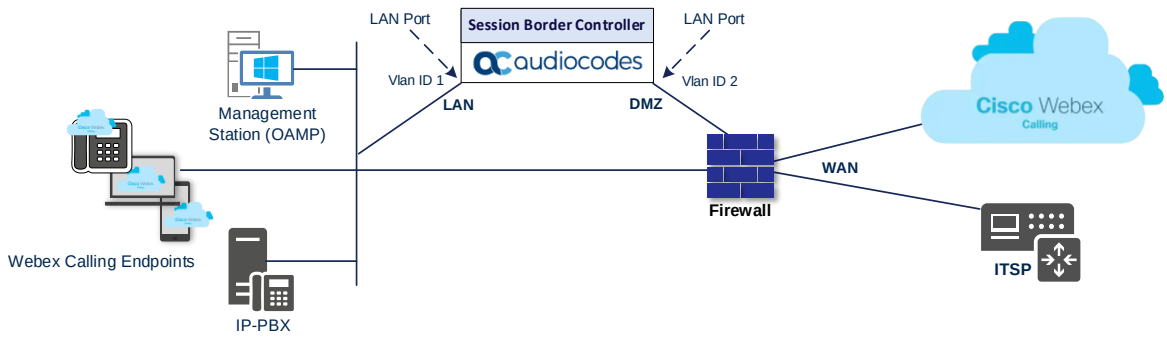
- FQDN published in the public DNS service, since this address must be resolvable from the Internet. The Administrator must be able to verify/claim their domain.
- Public certificate that is issued by one of the Cisco supported CAs. The certificate must contain the FQDN as a Common Name (CN) or Subject Alternative Name (SAN).

4.2 Configure IP Network Interfaces

This section describes how to configure the SBC's IP network interfaces. As mentioned in Section 2.4, 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:
  - Management Servers located on the LAN.
  - Cisco Webex Calling system and Audiocodes 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



4.2.1 Configure LAN and WAN VLANs

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

- LAN (assigned the name "LAN_IF")
- WAN (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**).

   There will be one existing row for VLAN ID 1 and underlying interface GROUP_1.
2. Add another VLAN ID 2 for the WAN side.

4.2.2 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	195.189.192.154 (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

4.2.3 (Optional) Configure NAT Translation

If the SBC is located in the Cloud, or just implemented with private IP addresses. The NAT Translation table lets you configure network address translation (NAT) rules for translating source IP addresses into NAT IP addresses (*global - public*), used in front of the Cloud or corporate firewall facing the Audiocodes SIP Trunk and the Cisco Webex Calling.

A NAT Translation Table is created automatically during the implementation of the Cloud based instance process. But if it's needed to configure manually, then follow the next steps.

To configure the NAT translation rules:

1. Open the NAT Translation table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **NAT Translation**).
2. Add a new NAT Translation rule by clicking **+New** at the top of the interface, and then configure the parameters using the table below as reference.

Table 4-2: NAT Translation Rule

Index	Source Interface	Source Start Port	Source End Port	Target IP Address	Target Start Port	Target End Port
0	eth0	1	65535	<Public IP Address>	1	65535

3. Click **Apply**.

4.3 Configure TLS Context for Cisco Webex Calling

This section describes how to configure the SBC for using a TLS connection with the Cisco Webex Calling System. This configuration is essential for a secure SIP TLS connection.

This certificate module is based on the DigiCert Certificate Chain. For more certificate structure options, refer to Cisco Webex Calling System documentation.

4.3.1 Configure the NTP Server Address

This section describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (local NTP server or another global NTP server) to ensure that the SBC receives the current date and time. This is necessary for validating certificates of remote parties. It is important, that the NTP Server is located on the OAMP IP Interface (LAN_IF in our case) or will be accessible through it.

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 first NTP server (e.g., **pool.ntp.org**).
3. In the 'Secondary NTP Server Address' field, enter the IP address of the second NTP server (e.g., **time2.google.com**).
4. Click **Apply**.

4.3.2 Create a TLS Context for Cisco Webex Calling System

This section describes how to request a certificate for the SBC WAN interface and configure it, based on the example of the DigiCert Global Root CA. The certificate is used by the SBC to authenticate the connection with the Cisco Webex Calling System.

The procedure involves the following main steps:

- Create a TLS Context for Cisco Webex Calling System
- Generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority (DigiCert in our example)
- Deploy the SBC and Root / Intermediate certificates on the SBC

To create a TLS Context for Cisco Webex Calling System:

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. Create a new TLS Context by clicking **+New**, and then configure the parameters using the table below as reference.

Table 4-3: New TLS Context

Index	Name	TLS Version
1	Cisco (arbitrary descriptive name)	TLSv1.2
All other parameters can be left unchanged with their default values.		

3. Click **Apply**; you should see the new TLS Context and option to manage the certificates at the bottom of 'TLS Context' table.

4.3.3 Generate a CSR and Obtain the Certificate from a Supported CA

This section describes how to generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority.

To generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority:

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the Cisco TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
3. Under the **Certificate Signing Request** group, do the following:
    a. In the 'Common Name [CN]' field, enter the SBC FQDN name (for example, **sbc.audiocodes.com**).
    b. In the '1st Subject Alternative Name [SAN]' field, change the type to 'DNS' and enter the SBC FQDN name (based on example above, **sbc.audiocodes.com**).
    c. Change the 'Private Key Size' based on the requirements of your Certification Authority. Many CAs do not support private key of size 1024.
    d. To change the key size on TLS Context, go to: **Generate New Private Key and Self-Signed Certificate**, change the 'Private Key Size' and then click **Generate Private-Key**. To use 2048 as a Private Key Size value, you can click **Generate Private-Key** without changing the default key size value.
    e. Fill in the rest of the request fields according to your security provider's instructions.
    f. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:
4. Copy the CSR from the line "**----BEGIN CERTIFICATE**" to "**END CERTIFICATE REQUEST----**" to a text file (such as Notepad), and then save it to a folder on your computer with an identifiable file name, for example, *certreq.txt*.
5. Send *certreq.txt* file to the Certified Authority Administrator for signing.

4.3.4 Deploy the SBC and Root / Intermediate Certificates on the SBC

After obtaining the SBC signed and Trusted Root/Intermediate Certificate from the CA, install the following:

- SBC certificate
- Root / Intermediate certificates

To install the SBC certificate:

1. In the SBC's Web interface, return to the TLS Contexts page and do the following:
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
   b. Scroll down to the Upload certificates files from your computer group, click the **Choose File** button corresponding to the 'Send Device Certificate...' field, navigate to the certificate file obtained from the CA, and then click **Load File** to upload the certificate to the SBC.
2. Validate that the certificate was uploaded correctly. A message indicating that the certificate was uploaded successfully is displayed in blue in the lower part of the page:
3. In the SBC's Web interface, return to the TLS Contexts page, select the required TLS Context index row, and then click the **Certificate Information** link, located at the bottom of the TLS. Then validate the Key size, certificate status and Subject Name.
4. In the SBC's Web interface, return to the TLS Contexts page.
   a. 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.
   b. Click the **Import** button, and then select all Root/Intermediate Certificates obtained from your Certification Authority to load.
5. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.

The above method creates a signed certificate for an explicit device, on which a Certificate Sign Request was generated (and signed with private key).

4.3.5 Deploy Cisco Trusted Root Certificate

Loading Cisco Trusted Root Certificates to AudioCodes' SBC is mandatory for implementing an MTLS connection with the Cisco Webex Calling network.

Download the certificate from the appropriated Certificate Authority website (DigiCert in our example) and follow the steps above to import it to the Trusted Root storage.

4.4 Configure Media Realms

This section describes how to configure Media Realms. Media Realms allows the dividing of the UDP port ranges for use on different interfaces. In the example below, two Media Realms are configured:

- One for the IP interface towards the Cisco Webex Calling System, with the UDP port starting at 20000 and the number of media session legs 100 (you need to calculate number of media session legs based on your usage).
- One for the IP interface towards Audiocodes SIP Trunk, with the UDP port range starting at 6000 and the number of media session legs 100.

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

Index	Name	IPv4 Interface Name	Port Range Start	Number of Media Session Legs
0	MR-Cisco (arbitrary name)	WAN_IF	20000	100 (media sessions assigned with port range)
1	MR-SIPTrunk (arbitrary name)	WAN_IF	6000	100 (media sessions assigned with port range)
All other parameters can be left unchanged at their default values.				

4.5 Configure SIP Signaling Interfaces

This section describes how to configure SIP Signaling Interfaces. A SIP Interface defines a listening port and type (UDP, TCP, or TLS) for SIP signaling traffic on a specific logical IP network interface (configured in the Interface Table above) and a Media Realm.

Note that the configuration of a SIP Interface for the Generic SIP Trunk is an example, your configuration might be different. For specific configuration of interfaces pointing to SIP trunks and/or a third-party PSTN environment connected to the SBC, see the trunk / environment vendor documentation.

AudioCodes also offers a comprehensive suite of documents covering the interconnection between different trunks and equipment.

To configure SIP Interfaces:

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

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

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Enable TCP Keepalive	Classification Failure Response Type	Media Realm	TLS Context Name	TLS Mutual Authentication
0	SI-Cisco (arbitrary name)	WAN_IF	SBC	0	0	5061[1]	Enable	0	MR-Cisco	Cisco	Enable
1	SI-SIPTrunk (arbitrary name)	WAN_IF	SBC	0	5067[2]	0	-	0[3]	MR-SIPTrunk	-	-
All other parameters can be left unchanged at their default values.											

[1] Port 5061 is mentioned as an example when any TLS port can be used.
[2] According to the Service Provider requirement.
[3] Recommended to prevent DoS attacks.

4.6 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:

- Cisco Webex Calling system
- Audiocodes SIP Trunk

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 4-6: Configuration Example Proxy Sets in Proxy Sets Table

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive	Redundancy Mode	Proxy Hot Swap	Proxy Load Balancing Method	DNS Resolve Method
1	Cisco-Webex (arbitrary name)	SI-Cisco	Cisco[4]	Using Options	Homing	Enable	Random Weights	SRV
2	SIPTrunk (arbitrary name)	SI-SIPTrunk	default	Using Options	According to SIP Trunk requirement	According to SIP Trunk requirement	According to SIP Trunk requirement	-

On Hybrid SBCs (with Onboard PSTN interfaces), it is recommended to leave Proxy Set 0 unconfigured for possible future use for PSTN Fallback.

[4] Configured in Section 4.3.2.

4.6.1 Configure a Proxy Address

This section describes how to configure a Proxy Address.

To configure a Proxy Address for Cisco-Webex Voice:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) click the Proxy Set **Cisco-Webex**, and then click the Proxy Address link located below the table; the Proxy Address table opens.
2. Click **+New** and configure the address of the Proxy Set according to the parameters described in the table below:

Table 4-7: Configuration Proxy Address for Cisco Webex Calling System

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	eun01.sipconnect.bcld.webex.com (as configured at Cisco Webex Admin Dashboard)	TLS	0	0

3. 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** and configure the address of the Proxy Set according to the parameters described in the table below:

Table 4-8: 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)	TCP	0	0

3. Click **Apply**.

4.7 Configure Coders

This section describes how to configure coders (termed *Coder Group*). The Cisco Webex Calling system supports OPUS coder. While the network connection to Audiocodes SIP Trunk may restrict operation with other dedicated coders listed (*e.g., G.729*), you need to add a Coder Group with the supported coders for each leg, for the Cisco Webex Calling system and for the Audiocodes SIP Trunk.

Note that the Coder Group ID for this entity is 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. From the 'Coder Group Name' dropdown, select **1:Does Not Exist** and add the required codecs as follows:

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711 U-law	20	64	0	Disabled
G.711 A-law	20	64	8	Disabled
Opus	20	N/A	111	N/A

3. Click **Apply** and confirm the configuration change in the prompt that pops up.

Repeat the same procedure for each Generic SIP Trunk if it's required.

The following procedure describes how to configure Allowed Audio Coders Groups to ensure that the voice sent to the Audiocodes SIP Trunk and Cisco Webex Calling system, uses the dedicated coders list whenever possible. Note that the Allowed Coders Group IDs will be assigned to the IP Profiles belonging to the Audiocodes SIP Trunk and Cisco Webex Calling system, in the next step.

To set a preferred coder for the Audiocodes 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 Audiocodes SIP Trunk (*e.g., SIPTrunk 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:

Index	Coder
0	G.729
1	G.711 U-law
2	G.711 A-law

To set a preferred coder for the Cisco Webex Calling system:

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 Cisco Webex Calling (e.g., *Cisco-Webex 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:

Index	Coder
0	G.711 U-law
1	G.711 A-law
2	Opus

6. Open the Media Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Settings**).
7. From the '**Extended Coders Behavior**' drop-down list, select **Include Extensions**.
8. Click **Apply**.

4.8 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).

To configure IP Profile for the Cisco Webex Calling system:

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **+New** and add the IP Profile for Cisco Webex Calling System interface. Configure the parameters using the table below as reference.

Table 4-9: Configuration Example: Cisco Webex Calling IP Profile

Parameter	Value
General	
Index	**1**
Name	**Cisco-Webex** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**Secured**
SBC Early Media	
Remote Early Media	**Not Supported** (relevant only if ICE mode is enabled)
SBC Media	
Extension Coders Group	**AudioCodersGroups_1**
Allowed Audio Coders	**Cisco-Webex Allowed Coders**
RFC 2833 Mode	**Extend**
ICE Mode	**Lite** (according to request)
SBC Signaling	
P-Asserted-Identity Header Mode	**Add**
Session Expires Mode	**Supported**
All other parameters can be left unchanged with their default values.	

3. Click **Apply**.

To configure an IP Profile for the Audiocodes SIP Trunk:

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **+New** to add the IP Profile for the Generic SIP Trunk. Configure the parameters using the table below as a reference.

Table 4-10: Configuration Example: Generic SIP Trunk IP Profile

Parameter	Value
General	
Index	**2**
Name	**SIPTrunk**
Media Security	
SBC Media Security Mode	**Not Secured**
SBC Media	
Extension Coders Group	**AudioCodersGroups_2**
Allowed Audio Coders	**SIPTrunk Allowed Coders**
Allowed Coders Mode	**Restriction and Preference** (reorder coders according to Allowed Coders including extension coders)
SBC Signaling	
P-Asserted-Identity Header Mode	**Add** (required for anonymous calls)

3. Click **Apply**.

4.9 Configure SIP Response Codes for Alternative Routing Reasons

This section describes how to configure the SBC's handling of SIP 503 responses received for outgoing SIP dialog-initiating methods, e.g., INVITE, OPTIONS, and SUBSCRIBE messages. In this case, the SBC attempts to locate an alternative route for the call. This feature works together with the Proxy Hot Swap feature, which is configured in the Proxy Sets table. Alternative routing based on SIP responses is configured using two tables with 'parent-child' relationships:

- Alternative Reasons Set table ('parent'): Defines the name of the Alternative Reasons Set.
- Alternative Reasons Rules table ('child'): Defines SIP response codes per Alternative Reasons Set.

To apply your configured alternative routing reason rules, you need to assign the Alternative Reasons Set for which you configured the rules, to the Cisco Webex Calling IP Group in the IP Groups table, using the 'SBC Alternative Routing Reasons Set' parameter.

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 Set**).
2. Click New**,** and then configure a name for the Alternative Routing Reasons Set (e.g., *Cisco Alternative Reasons*).
3. Click **Apply**.
4. Select the index row of the Alternative Reasons Set that you added, and then click the Alternative Reasons Rules link located at the bottom of the page; the Alternative Reasons Rules table opens.
5. Click **New** and select **503 Service Unavailable** from the 'Release Cause Code' drop-down list.
6. Click **Apply**.

4.10 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:

- Cisco Webex Calling system
- Audiocodes SIP Trunk

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 Cisco Webex Calling system:

Parameter	Value
Name	**Cisco-Webex** (arbitrary descriptive name)
Type	**Server**
Proxy Set	**Cisco-Webex**
IP Profile	**Cisco-Webex**
Media Realm	**MR- Cisco**
SIP Group Name	**eun01.sipconnect.bcld.webex.com** (according to Cisco Webex Admin Dashboard configuration)
SBC Alternative Routing Reason Set	**Cisco Alternative Reasons** (as configured in the previous section)
Proxy Keep-Alive using IP Group settings	**Enable**
All other parameters can be left unchanged with their default values.	

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

Parameter	Value
Index	**1**
Name	**SIPTrunk** (arbitrary descriptive name)
Type	**Server**
Proxy Set	**SIPTrunk**
IP Profile	**SIPTrunk**
Media Realm	**MR-SIPTrunk**
All other parameters can be left unchanged with their default values.	

4.11 Configure SRTP

This section describes how to configure media security. The Cisco Webex Calling System Interface uses SRTP only, so you need to configure the SBC to operate in the same manner. By default, SRTP is disabled.

To configure media security:

1. Open the Media Security page (**Setup menu > Signaling & Media tab > Media folder > Media Security**).
2. From the '**Media Security**' drop-down list, select **Enable** to enable SRTP.
3. Click **Apply**.

4.12 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 Cisco Webex Calling system and Audiocodes SIP Trunk:

- Terminate SIP OPTIONS messages on the SBC that are received from any entity
- Calls from Cisco Webex Calling system to Audiocodes SIP Trunk
- Calls from Audiocodes SIP Trunk to Cisco Webex Calling system

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 4-11: 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	Cisco to ITSP (arbitrary name)	Cisco-Webex		IP Group	SIPTrunk	
2	ITSP to Cisco (arbitrary name)	SIPTrunk		IP Group	Cisco-Webex	

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

4.13 Configure Number Manipulation Rules (Optional)

This section describes how to configure IP-to-IP number 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 4.9 on page 21) to denote the source and destination of the call.

> Adapt the manipulation table according to your environment dial plan.

For example, for this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination number (if it does not exists) for calls from the Audiocodes SIP Trunk IP Group to the Cisco Webex Calling system IP Group for any destination username pattern.

To configure a number manipulation rule:

1. Open the Outbound Manipulations table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Manipulation** > **Outbound Manipulations**).
2. Configure the rules according to your setup.

The table below is an example of configured IP-to-IP outbound manipulation rules for calls between the Cisco Webex Calling system IP Group and Audiocodes SIP Trunk IP Group:

Rule Index	Description
0	Calls from SIP Trunk IP Group to Cisco-Webex IP Group with any destination number between 1 to 9, add "+" to the prefix of the destination number.

4.14 Configure Message Manipulation Rules

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 or SIP Interface (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

To configure SIP message manipulation rule for Cisco Webex Calling:

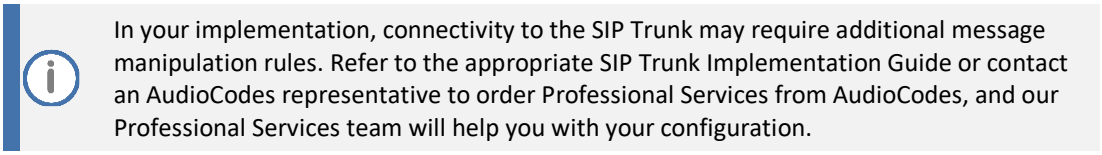
1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 0) for Cisco Webex Calling. This rule applies to the SIP OPTIONS messages received from the Cisco Webex Calling. Cisco send SIP OPTIONS messages with the Max-Forwards header value '0', which cause to error messages in the syslog. This rule modifies the value of the Max-Forwards header with value '70'.

Parameter	Value
Index	**0**
Name	**Change Max-Forwards** (arbitrary name)
Manipulation Set ID	**0**
Message Type	**Options.Request**
Condition	**Header.Max-Forwards=='0'**
Action Subject	**Header.Max-Forwards**
Action Type	**Modify**
Action Value	**'70'**

3. Configure another manipulation rule (Manipulation Set 2) for the Cisco Webex Calling IP Group. This rule applies to messages sent to the Cisco Webex Calling IP Group. This rule replaces the host part of the SIP Contact header with the 'sbc.webex.aceducation.info' value as required by Cisco.

Parameter	Value
Index	**1**
Name	**Change Contact** (arbitrary name)
Manipulation Set ID	**2**
Message Type	**Any**
Action Subject	**Header.Contact.URL.Host**
Action Type	**Modify**
Action Value	**'sbc.webex.aceducation.info'**

4. Assign Manipulation Set ID 0 to the Cisco Webex Calling SIP Interface:
   a. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
   b. Select the row of the Cisco Webex Calling SIP Interface, and then click **Edit**.
   c. Set the 'Pre-classification Manipulation Set ID' field to **0**.
   d. Click **Apply**.
5. Assign Manipulation Set ID 2 to the Cisco Webex Calling IP Group:
   a. Open the IP Groups table (Setup menu > Signaling & Media tab > Core Entities folder > IP Groups).
   b. Select the row of the Cisco Webex Calling IP Group, and then click **Edit**.
   c. Set the 'Outbound Message Manipulation Set' field to **2**.
   d. Click **Apply**.



In your implementation, connectivity to the SIP Trunk may require additional message manipulation rules. Refer to the appropriate SIP Trunk Implementation Guide or contact an AudioCodes representative to order Professional Services from AudioCodes, and our Professional Services team will help you with your configuration.

4.15 Configure Registration Accounts (Optional)

This section describes how to configure SIP registration accounts. This is required so that the SBC can register with the Audiocodes SIP Trunk on behalf of the Cisco Webex Calling system. The Audiocodes SIP Trunk requires registration and authentication to provide service.

In our example, the Served IP Group is Cisco Webex Calling system IP Group and the Serving IP Group is Audiocodes SIP Trunk IP Group.

Configure Registration Account only if this is required by the SIP Trunk.

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, for example:

Parameter	Value
Served IP Group	**Cisco-Webex**
Application Type	**SBC**
Serving IP Group	**SIPTrunk**
Host Name	As provided by the SIP Trunk provider
Register	**Regular**
Contact User	**123456789** (trunk main line)
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

4. Click **Apply**.

4.16 Configure Firewall Settings (Optional)

As an additional security measure, there is an option to configure traffic filtering rules (access list) for incoming traffic on AudioCodes SBC. For each packet received on the configured network interface, the SBC searches the table from top to bottom until the first matching rule is found. The matched rule can permit (allow) or deny (block) the packet. Once a rule in the table is located, subsequent rules further down the table are ignored. If the end of the table is reached without a match, the packet is accepted. Please note that the firewall is stateless. The blocking rules will apply to all incoming packets, including UDP or TCP responses.

To configure a firewall rule:

1. Open the Firewall table (**Setup** menu > **IP Network** tab > **Security** folder> **Firewall**).
2. Configure the following Access list rules for WAN IP Interface, based on the list of Cisco Webex Calling System Servers:

Table 4-12: Firewall Table Rules

Index	Source IP	DNS Query Type	Prefix Length	Start Port	End Port	Protocol	Use Specific Interface	Interface ID	Allow Type
0	<Public DNS Server IP> (e.g., 8.8.8.8)	-	32	0	65535	Any	Enable	WAN_IF	Allow
1	eun01.sipconnect.bcld.webex.com	SRV	-	0	65535	Any	Enable	WAN_IF	Allow
2	<SIP Trunk server 1>	-	32	0	65535	TCP	Enable	WAN_IF	Allow
3	<SIP Trunk server 2>	-	32	0	65535	TCP	Enable	WAN_IF	Allow
49	0.0.0.0	-	0	0	65535	Any	Enable	WAN_IF	Block

Be aware, that if in your configuration, connectivity to SIP Trunk (or other entities) is performed through the same IP Interface as Cisco Webex Calling (WAN_IF in our example), you must add rules to allow traffic from these entities. See an example in rows 2 and 3.

4.17 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

4.17.1 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.

> If your SBC is deployed in a virtual environment and transcoding is required, your virtual machine must have a minimum of 2 vCPUs. For more information, please refer to the appropriate Installation Manual, which can be found on the AudioCodes website.

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

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
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-12732