Configuration Note

AudioCodes Professional Services – Interoperability Lab

Avaya Aura® Platform Release 8.1.x and Generic SIP Trunk using AudioCodes Mediant™ SBC

Version 7.2

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: 16-April-2020

WEEE EU Directive

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

Customer Support

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

Stay in the Loop with AudioCodes

Abbreviations and Terminology

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

Document Revision Record

LTRT	Description
12265	Initial document release for Version 7.2.

Documentation Feedback

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

This page is intentionally left blank.

1 Introduction

This Configuration Note describes how to set up the AudioCodes Enterprise Session Border Controller (hereafter, referred to as *SBC*) for interworking between Generic's SIP Trunk and Avaya Aura Platform Release 8.1.x 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 Web site at https://www.audiocodes.com/partners/sbc-interoperability-list.

1.1 Intended Audience

This document is intended for engineers, or AudioCodes and Generic partners who are responsible for installing and configuring Generic's SIP Trunk and Avaya's Aura Platform Release 8.1.x for enabling VoIP calls using AudioCodes SBC.

1.2 About AudioCodes SBC Product Series

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

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

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

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

1.3 About Avaya Aura Platform

Avaya Aura is a communications solution that uses an IP and SIP-based architecture to unify media, modes, networks, devices, applications, and real-time, actionable presence across a common infrastructure. This architecture provides on-demand access to advanced collaboration services and applications that improve employee efficiency. Avaya Aura is available under Core or Power Suite Licenses. Each suite provides a customized set of capabilities designed to meet the needs of different kinds of users. Customers might mix Core and Power licenses on a single system based on their needs.

Avaya Aura Platform comprises: Communication Manager, Session Manager, Session Border Controller for Enterprise, System Manager, Messaging, Communication Manager Messaging, Application Enablement Services (AE Services) and the Presence Services Snap-in.

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes SBC Version

Table 2-1: AudioCodes SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500L Gateway & E-SBC ▪ Mediant 500 Gateway & E-SBC ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 800C Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC ▪ Mediant 4000B SBC ▪ Mediant 9000 SBC ▪ Mediant 9030 SBC ▪ Mediant 9080 SBC ▪ Mediant Software SBC (VE/SE/CE)
Software Version	7.20A.254.202 or later
Protocol	▪ SIP/TLS (to both the Generic SIP Trunk and Avaya Aura)
Additional Notes	None

2.2 Avaya Aura Platform Components and Version

Table 2-2: Avaya Aura Platform Components and Version

Vendor	Avaya
Model	Session Manager, Communication Manager, System Manager, Media Server, 450 Media Gateway
Software Version	8.1.x
Protocol	SIP
Additional Notes	None

2.3 Generic SIP Trunking Version

Table 2-3: Generic Version

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

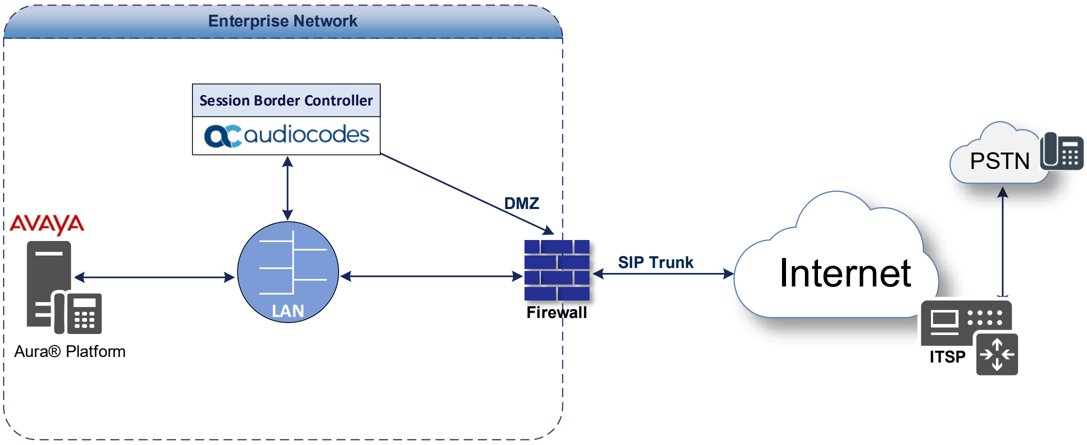
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes SBC and Generic SIP Trunk with Avaya Aura Platform was done using the following topology setup:

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

The figure below illustrates this interoperability test topology:

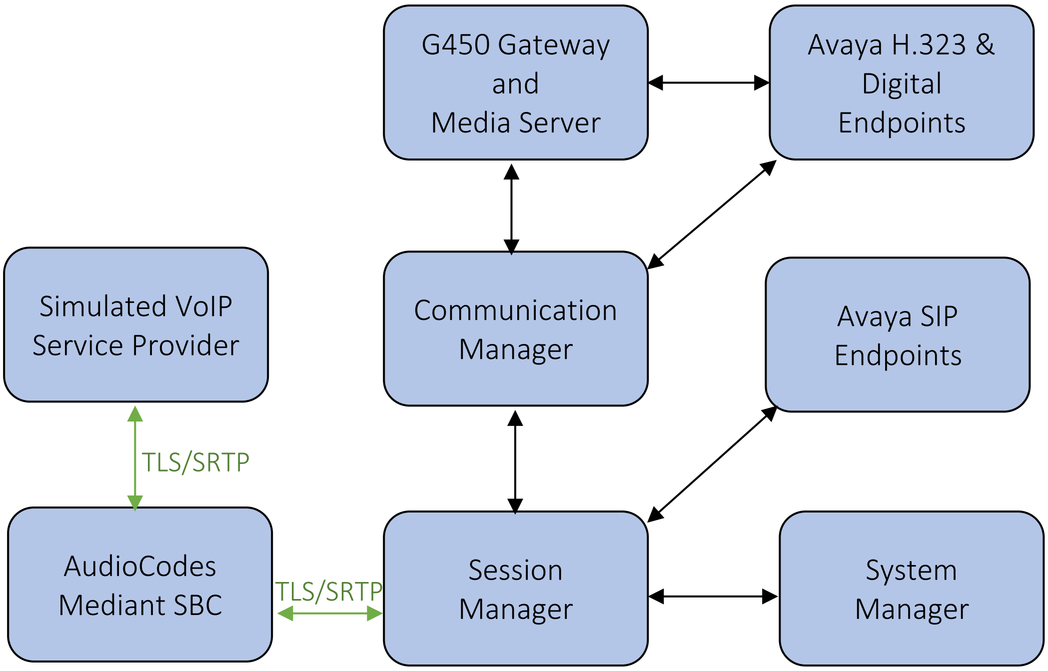
Figure 2-1: Interoperability Test Topology between Avaya Aura Platform and Generic SIP Trunk using SBC



2.4.1 Avaya Aura Platform Reference Configuration

The reference configuration consists of Communication Manager, Session Manager, System Manager, Messaging, AudioCodes Mediant SBC, and a number of Avaya telephones. AudioCodes Mediant SBC is used as a SIP/ISDN gateway for PSTN access. The Session Manager in the bottom-middle block, managed through the System Manager in the bottom-right block, routes the calls between the different entities using SIP Trunks. The management interface of AudioCodes Mediant SBC has to be on a different subnet from the signaling and media interfaces. The Messaging server resides in another subnet and is connected to the Communication Manager via a different Session Manager (not shown).

Figure 2-2: Sample configuration for Avaya Aura Communication Manager and Avaya Aura Session Manager with AudioCodes Mediant SBC using SIP Trunking



2.4.2 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	▪ Avaya Aura Platform is located on the LAN ▪ Generic SIP Trunk is located on the WAN
Signaling Transcoding	▪ Both Avaya Aura Platform and generic SIP trunk operates with SIP-over-TLS transport type
Codecs Transcoding	▪ Both, Avaya Aura Platform and generic SIP trunk supports G.711A-law and G.711U-law coders
Media Transcoding	▪ Both, Avaya Aura Platform and generic SIP trunk operates with SRTP media type

2.4.3 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes SBC interworking between Avaya Aura Platform and Generic's SIP Trunk.

3 Configure Avaya Aura Platform

This section describes how to configure Avaya Aura Platform.

3.1 Configure Avaya Aura Communication Manager

This section describes how to configure Avaya Aura 8.1.x Communication Manager to operate with AudioCodes SBC.

Note: For more complicated configuration parameters please refer to Avaya Aura 8.1.x Communication Manager documentation.

The following procedures are described in this chapter:

- Verify Avaya Aura Communication Manager License (see Section 3.1.1)
- Configure IP Node Names (see Section 3.1.2)
- Configure IP Codec Set (see Section 3.1.3)
- Configure IP Network Region (see Section 3.1.4)
- Configure SIP Trunks with Session Manager (see Section 3.1.5)
- Configure Route Pattern (see Section 3.1.6)
- Configure Private Unknown Numbering (see Section 3.1.7)
- Administer ARS Analysis (see Section 3.1.8)
- Administer Feature Access Code (see Section 3.1.9)

Throughout this section the administration of Communication Manager is performed using a System Access Terminal (SAT). Some administration screens have been abbreviated for clarity. These instructions assume that the Communication Manager has been installed, configured, licensed and provided with a functional dial plan. In these Application Notes, Communication Manager was configured with 5-digit extension **7xxxx** for IP and SIP stations and **53xxx** for PSTN access via AudioCodes Mediant SBC.

3.1.1 Verify Avaya Aura Communication Manager License

You need to verify that there are sufficient licenses for managing SIP Trunks.

➢ **Do the following:**

1. Enter the display system-parameters customer-options command.
2. Navigate to **Page 2** and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

   If there is insufficient capacity of SIP Trunks or a required feature is not enabled, contact an Avaya representative to make the appropriate changes.

```
display system-parameters customer-options                        Page   2 of  12

                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                 USED
                 Maximum Administered H.323 Trunks: 12000          0
       Maximum Concurrently Registered IP Stations:  2400          1
         Maximum Administered Remote Office Trunks: 12000          0
Max Concurrently Registered Remote Office Stations:  2400          0
          Maximum Concurrently Registered IP eCons:  128           0
     Max Concur Reg Unauthenticated H.323 Stations:   100          0
                    Maximum Video Capable Stations:  36000         0
               Maximum Video Capable IP Softphones:   2400         0
                   Maximum Administered SIP Trunks: 12000         10
  Max Administered Ad-hoc Video Conferencing Ports: 12000          0
   Max Number of DS1 Boards with Echo Cancellation: 688        0
```

3.1.2 Configure IP Node Names

All calls with the Communication Manager are signaled over a SIP trunk to Session Manager. The signaling interface on the Session Manager is provided by the SM100 security module. Use the **change node-names ip** command to add the **Name** and **IP Address** for the SIP security module of Session Manager. In the example below, **sm81** and **10.64.110.212** were used.

```
change node-names ip                                              Page   1 of   2

                                  IP NODE NAMES
    Name                IP Address
aes81                 10.64.110.215
ams81                 10.64.110.214
cms19                 10.64.110.225
default               0.0.0.0
procr                 10.64.110.213
procr6                ::
sm81                  10.64.110.212
```

3.1.3 Configure IP Codec Set

Use the **change ip-codec-set n** command to specify **G.711MU** and **G.729** codecs under **Audio Codec** where **n** is the codec set used in the configuration. Configure the **Media Encryption** and **Encrypted SRTCP** as shown below.

```
change ip-codec-set 1                                            Page   1 of   2

                           IP MEDIA PARAMETERS
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n          2        20
 2: G.729             n          2        20
 3:
 4:
 5:
 6:
 7:

     Media Encryption                  Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: 2-srtp-aescm128-hmac32
 3:
 4:
 5:
```

3.1.4 Configure IP Network Region

This section describes the IP network regional settings using the **change ip-network-region n** command, where **n** is the number of the network regions used.

➢ **Do the following:**

1. Set the **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** fields to **yes**.
2. For **Codec Set,** enter the codec set configured in Section 3.1.3. Set the **Authoritative Domain** to **avaya.com**. Retain the default values for the remaining fields.

```
change ip-network-region 1                                       Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location:          Authoritative Domain: avaya.com
    Name:                         Stub Network Region: n
MEDIA PARAMETERS                  Intra-region IP-IP Direct Audio: yes
      Codec Set: 1                Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                        IP Audio Hairpinning? y
   UDP Port Max: 3329
```

3.1.5 Configure SIP Trunk with Avaya Aura Session Manager

To administer a SIP Trunk on Communication Manger, two intermediate steps are required, creation of a signaling group and of a trunk group.

3.1.5.1 Configure Signaling Group

Use the **add signaling-group n** command, where **n** is an available signaling group number, and fill in the indicated fields.

- Group Type: sip
- Transport Method: tls
- Near-end Node Name: procr
- Far-end Node Name: Session Manager node name from Section 3.1.2
- Near-end Listen Port: 5061
- Far-end Listen Port: 5061
- Far-end Network Region: 1
- Far-end Domain: avaya.com
- DTMF over IP: rtp-payload (or in-band or out-of-band)

Default values can be used for the remaining fields.

```
add signaling-group 1                                              Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1             Group Type: sip
  IMS Enabled? n       Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? n
   Peer Detection Enabled? y  Peer Server: SM                       Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n

   Near-end Node Name: procr                    Far-end Node Name: sm1
 Near-end Listen Port: 5061                   Far-end Listen Port: 5061
                                           Far-end Network Region: 1
                                      Far-end Secondary Node Name:
Far-end Domain: avaya.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Initial IP-IP Direct Media? n
```

3.1.5.2 Configure SIP Trunk Group

This section describes how to configure the SIP Trunk Group.

➢ **Do the following:**

1. Add the corresponding trunk group controlled by the above signaling group via the **add trunk-group n** command, where **n** is an available trunk group number and fill in the indicated fields.
   - Group Type: **sip**
   - Group Name: A descriptive name (e.g. **SM Trunk**)
   - TAC: An available trunk access code (e.g. **101**)
   - Service Type: **tie**
   - Signaling Group: Number of the signaling group added in Section **3.1.5.1** (i.e. **1**)
   - Number of Members: The number of SIP trunks to be allocated to calls routed to Session Manager (must be within the limits of the total trunks available licensed).

```
add trunk-group 1                                             Page   1 of   5
                                TRUNK GROUP

Group Number: 1                   Group Type: sip          CDR Reports: y
  Group Name: SM Trunk                   COR: 1        TN: 1        TAC: 101
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                      Member Assignment Method: auto
                                               Signaling Group: 1
                                             Number of Members: 10
```

2. Navigate to **Page 3** and change **Numbering Format** to **private.** Use default values for all other fields.

```
add trunk-group 1                                               Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                   Maintenance Tests? y



                     Numbering Format: private
                                                 UUI Treatment: shared
                                              Maximum Size of UUI Contents: 128
                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                                                  Hold/Unhold Notifications? y
                                 Modify Tandem Calling Number: no
```

3.1.6 Configure Route Patterns

Configure a route pattern to correspond to the newly added SIP trunk group. Use **change route pattern n** command, where **n** is an available route pattern. When changing the route pattern, enter the following values for the specified fields:

- **Grp No:** The trunk group number from **Section 3.1.5.2**
- **FRL:** Enter a level that allows access to this trunk, with **0** being least restrictive

Retain the default values for the remaining fields.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1      Pattern Name:
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1:  1   0                                                              n   user
 2:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                          none
 2: y y y y y n  n            rest                                          none
```

3.1.7 Configure Private Numbering

Use the **change private-numbering 0** command to assign the number displayed by the Communication Manager for calls sent to the Session Manager. Add an entry for the Extensions configured in the dial plan. Enter the following values for the specified fields:

- **Ext Len:** Number of digits of the Extension i.e. **5**
- **Ext. Code:** Leading digits of the Extension number, i.e. **7**
- **Trk Group:** Leave it blank (meaning any trunk)
- **CPN Prefix:** Leave it blank
- **Total CPN Len:** Total number of digits i.e. **5**

Retain default values for the remaining fields.

```
change private-numbering 0                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext                  Trk         Private          Total
Len Code                 Grp(s)      Prefix           Len
 5  5                                                 5  Total Administered: 2
 5  7                                                 5     Maximum Entries: 540
```

3.1.8 Administer ARS Analysis

This section shows a sample Auto Route Selection (ARS) entry used for routing calls with dialed digits beginning with **53**. Use the **change ars analysis 53** command to add an entry and specify how to route calls. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Dialed String:** Dialed prefix digits to match on, in this case **53**
- **Total Min:** Minimum number of digits, in this case **5**
- **Total Max:** Maximum number of digits, in this case **4**
- **Route Pattern:** The route pattern number from Section **3.1.6,** i.e. **1**
- **Call Type:** **hnpa**

Note that additional entries may be added for different number destinations.

```
change ars analysis 1720                                        Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 0

          Dialed              Total     Route     Call   Node   ANI
          String             Min  Max  Pattern    Type   Num    Reqd
    53                       5    5     1         hnpa          n
```

3.1.9 Administer Feature Access Code

Use the **change feature access code** command to define a feature access code for **Auto Route Selection (ARS).** In the test, **9** was used.

```
change feature-access-codes                                     Page   1 of  11
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
```

3.2 Configure Avaya Aura Session Manager

This section describes the procedures for configuring the Session Manager, assuming it has been installed and licensed.

> **Note:** This section only covers the basic configuration. For more complex configuration, refer to Avaya Aura Platform documentation.

Calls to and from the VoIP Service provider are routed via AudioCodes Mediant SBC. The procedures are described in this section:

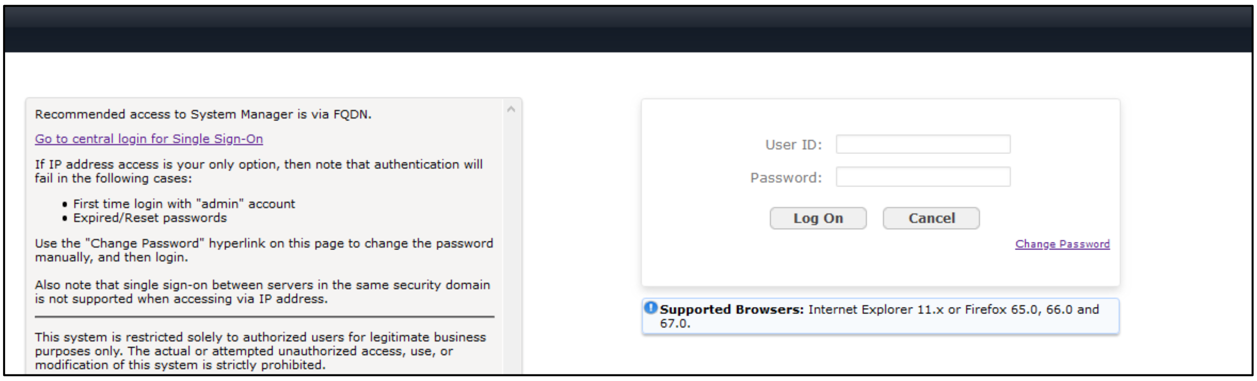
- Specify SIP Domain (see Section 3.2.1)
- Add Locations (see Section 3.2.2)
- Add SIP Entities (see Section 3.2.3)
- Add Entity Links (see Section 3.2.4)
- Add Routing Policies (see Section 3.2.5)
- Add Dial Patterns (see Section 3.2.6)

It is assumed that the following items that are required for SIP stations configuration have been configured. These items are not described in this section:

- Communication Manager as an Application
- Application Sequence Configuration
- Users for SIP Stations

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials. The menu shown below is displayed:

Figure 3-1: Avaya Aura System Manager



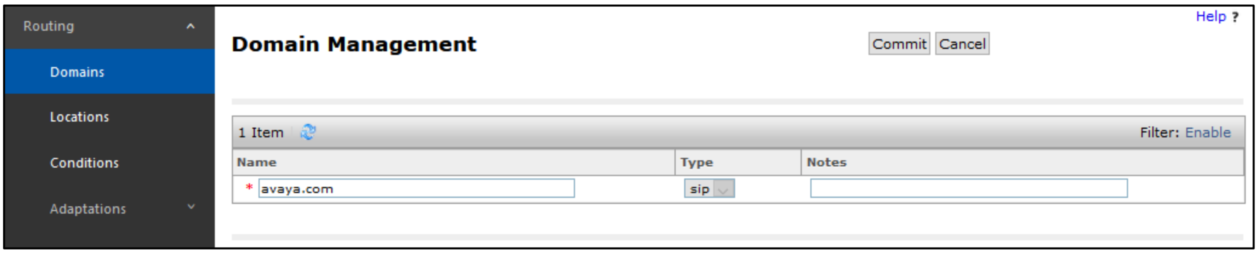
3.2.1 Specify SIP Domain

This section describes how to specify the SIP domain.

➢ **Do the following:**

1. Once logged on, navigate to Add the SIP domain for which the communications infrastructure will be authoritative.
2. In the Navigation pane, select **Domains**, and then click **New**. The following screen is displayed.

Figure 3-2: Domain Management



3. Fill in the following fields and click **Commit**.
   - **Name:** The authoritative domain name (e.g. **avaya.com**)
   - **Type:** Select sip
   - **Notes:** Descriptive text (optional)

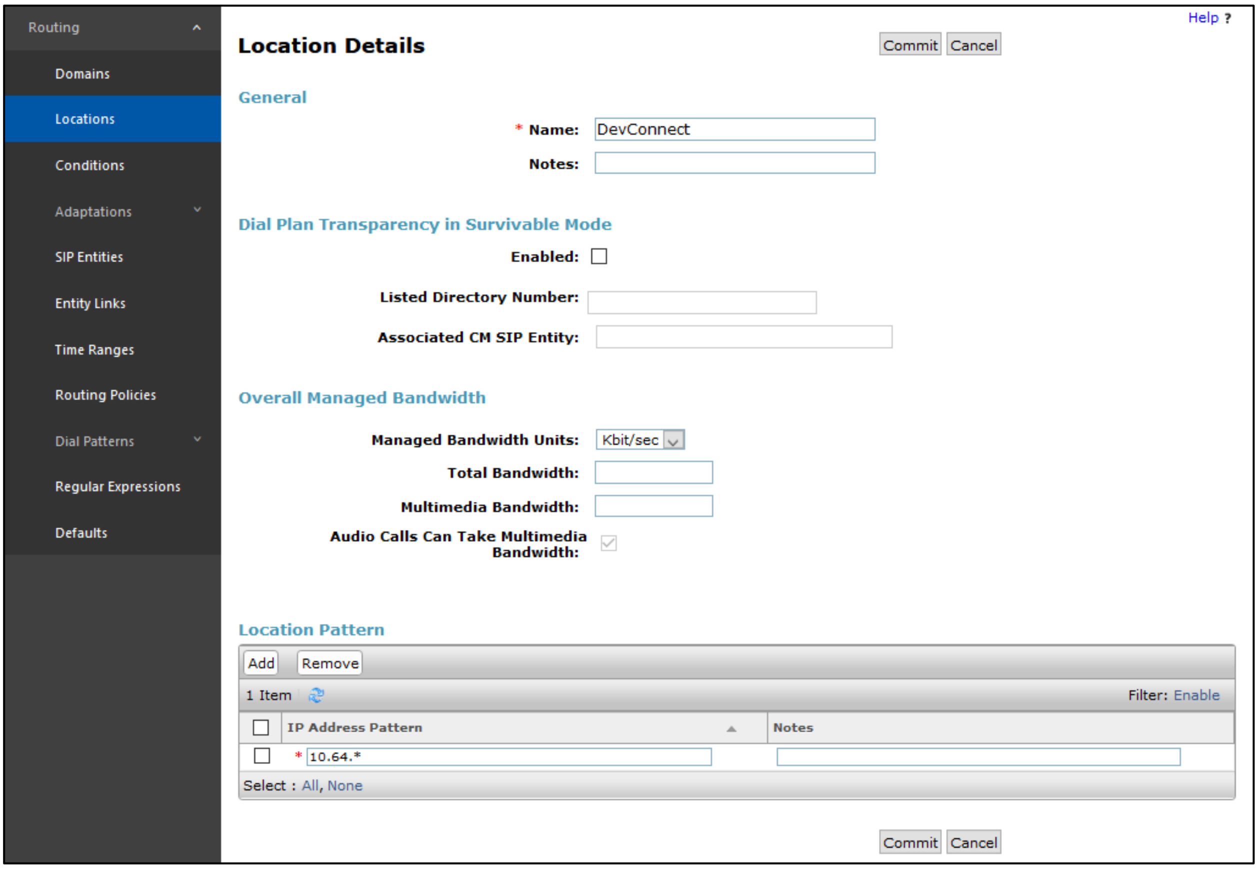
3.2.2 Add Locations

Locations can be used to identify logical and/or physical locations where SIP entities reside for the purpose of bandwidth management. A single location is added to the configuration for Communication Manager and AudioCodes Mediant SBC.

➢ **To add a location:**

1. In the Navigation pane select **Locations**, and then click **New**.
2. Fill in the following fields:
   - Under **General**:
     - **Name:** A descriptive name
     - **Notes:** Descriptive text (optional)
   - Under Location Pattern:
     - **IP Address Pattern:** A pattern used to logically identify the location. In these Application Notes, the pattern represented the networks involved, i.e. **10.64.***.
     - **Notes:** Descriptive text (optional)
3. Click **Commit** to save.

Figure 3-3: Location Details



3.2.3 Add SIP Entities

A SIP entity must be added for the Communication Manager and for AudioCodes Mediant SBC connected for SIP trunking to VoIP Service Provider.

3.2.3.1 Adding Avaya Aura Communication Manager

This section describes how to add the Avaya Aura Communication Manager.

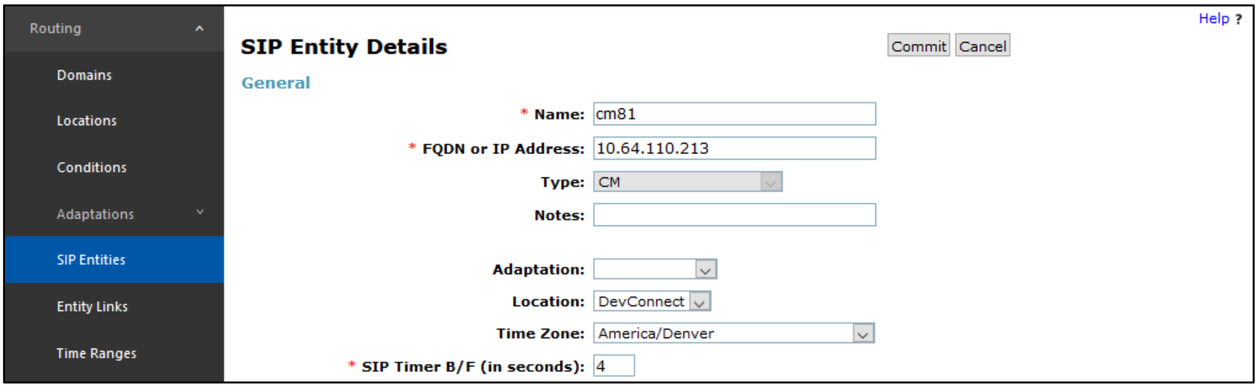
➢ **Do the following:**

1. In the Navigation pane, select **SIP Entities** and then click **New**.
2. Under **General,** fill in the following fields:
   - **Name:** A descriptive name
   - **FQDN or IP Address:** IP address of the procr interface of Communication Manager, i.e. **10.64.110.213**
   - **Type:** Select **CM**
   - **Location:** Select the location defined in Section 3.2
   - **Time Zone:** Time zone for this entity

   Defaults can be used for the remaining fields.

3. Click **Commit** to save the SIP entity definition.

Figure 3-4: SIP Entity Details- Avaya Aura Communication Manager



3.2.3.2 Adding AudioCodes Mediant SBC

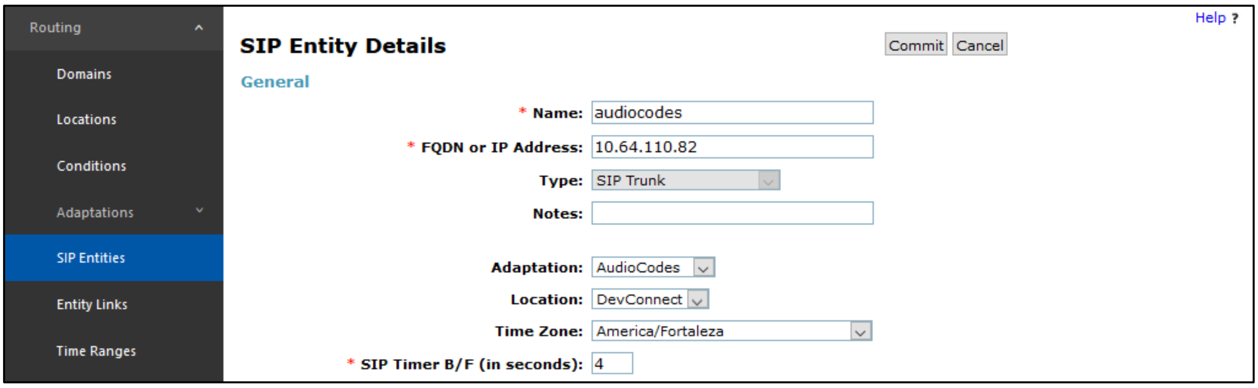
This section describes how to add an AudioCodes Mediant SBC.

➢ To add an AudioCodes Mediant SBC:

1. In the Navigation pane, select **SIP Entities** and then click **New**.
2. Under **General**, fill in the following fields:
   - **Name:** A descriptive name
   - **FQDN or IP Address:** IP address of the private signaling interface of AudioCodes Mediant SBC, i.e. **10.64.110.82**
   - Type: Select SIP Trunk
   - **Location:** Select the location defined in Section 3.2
   - **Time Zone:** Time zone for this entity

   Defaults can be used for the remaining fields.
3. Click **Commit** to save the SIP entity definition.

Figure 3-5: SIP Entity Details-SBC



3.2.4 Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an entity link.

➢ **To add an entity link:**

1. In the Navigation pane, select **Entity Links** and then click **New**.
2. Fill in the following fields in the new row that is displayed:
   - **Name:** A descriptive name
   - **SIP Entity 1:** Select the Session Manager SIP Entity
   - **Port:** Port number to which the far end system sends SIP requests
   - **SIP Entity 2:** Select the name of the far end system
   - **Port:** Port number on which the far end system receives SIP requests
   - **Trusted:** Check this box, otherwise calls from the SIP Entity specified will be denied (not shown)
   - **Protocol:** Select the transport protocol to align with the far end. In these Application Notes **TLS** was used for Communication Manager and for AudioCodes Mediant SBC
3. Click **Commit** to save each entity link definition.

Figure 3-6: Entity Links

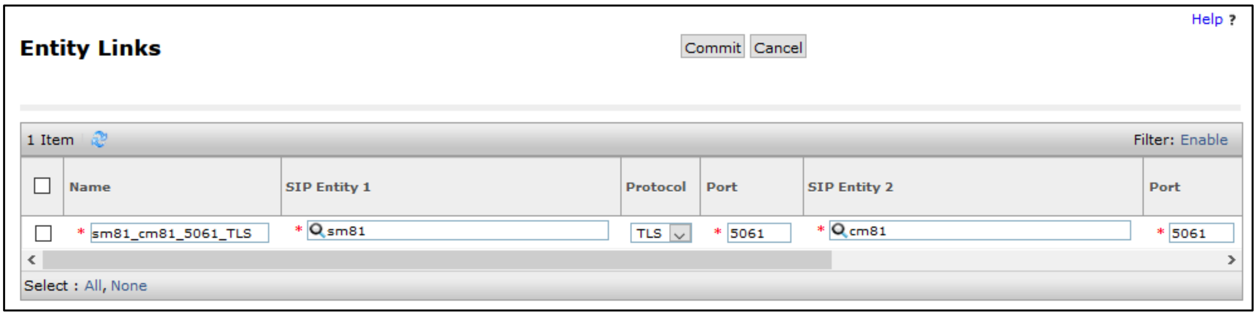
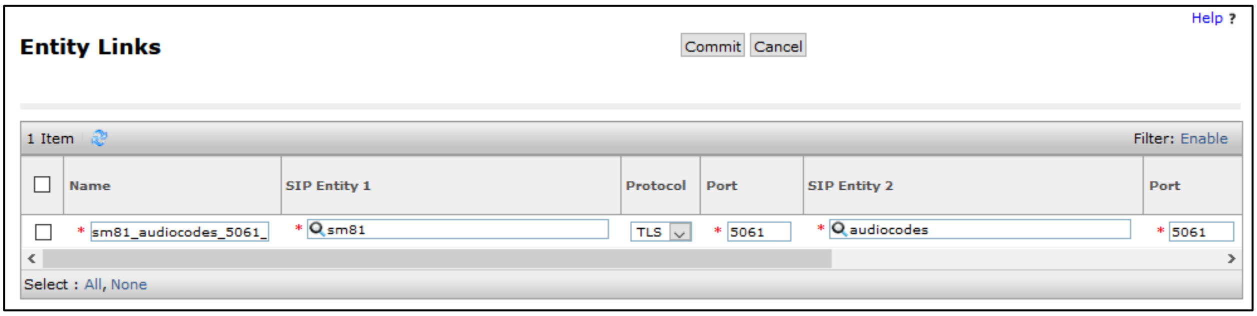


Figure 3-7: Entity Link for AudioCodes Mediant SBC



3.2.5 Add Routing Policies

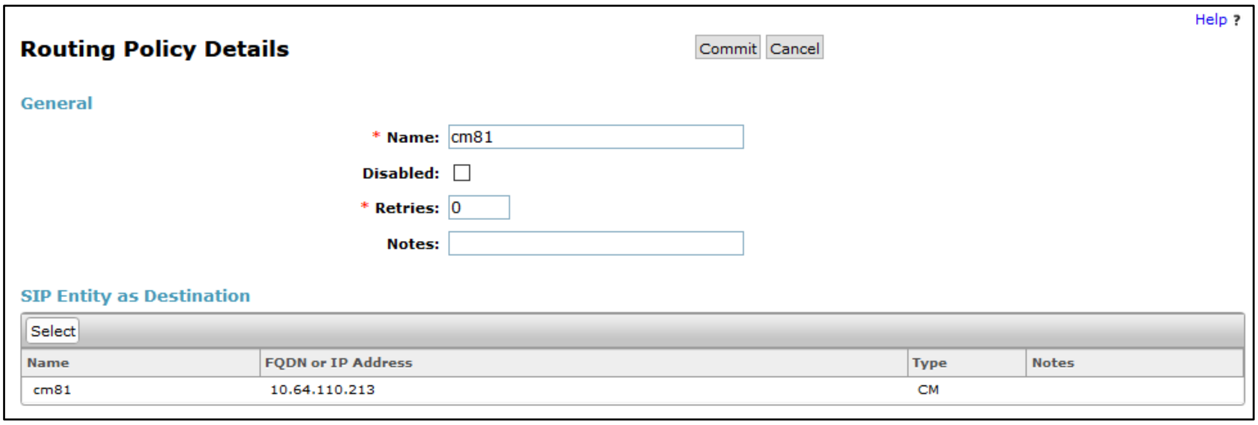
Routing policies describe the condition under which calls are routed to the SIP Entities specified in Section 3.2.3. Two routing policies are added: one for the Communication Manager and another for the AudioCodes Mediant SBC.

➢ **To add a routing policy:**

1. In the Navigation pane, select **Routing Policies** and then click the **New** .
2. Under **General**, enter a descriptive name in **Name**.
3. Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity to which this routing policy applies (not displayed).

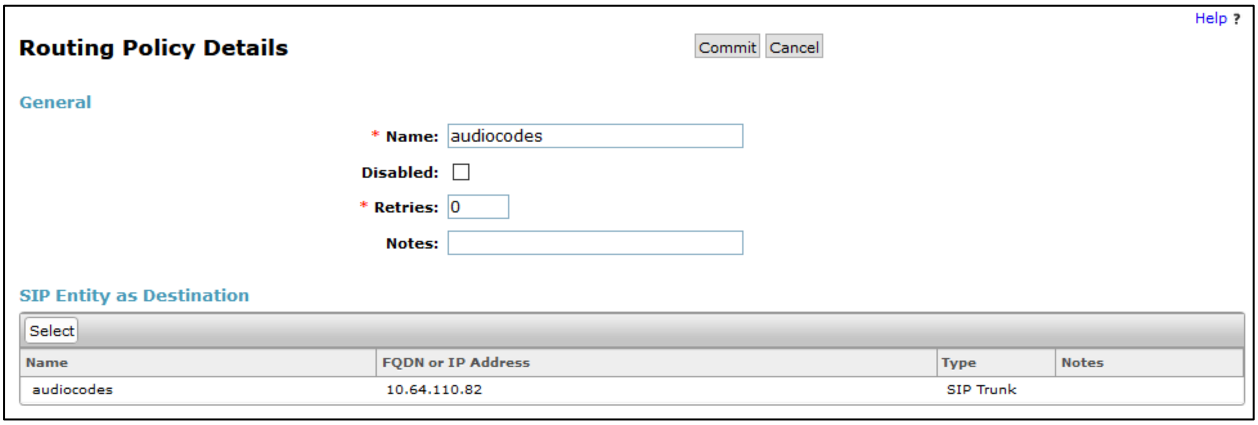
   Defaults can be used for the remaining fields.
4. Click **Commit** to save each Routing Policy definition.

Figure 3-8: Routing Policy Details



The following screen shows the Routing Policy for AudioCodes Mediant SBC.

Figure 3-9: Routing Policy Details: SBC



3.2.6 Add Dial Patterns

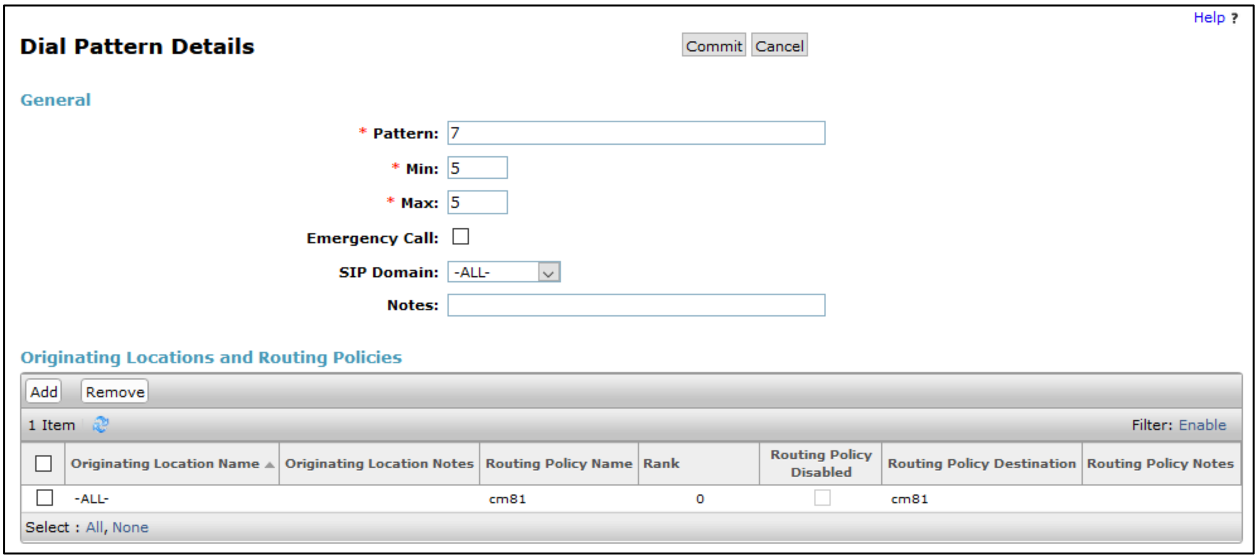
Dial patterns must be defined that direct calls to the appropriate SIP entity. Fill in the following fields as specified for the dial pattern that routes calls to Communication Manager.

- **To add a dial pattern:**

1. In the Navigation pane, select **Dial Patterns** and then click **New**.
2. Under **General**:
   - **Pattern:** Dialed number or prefix, **7**
   - **Min:** Minimum length of dialed number, **5**
   - **Max:** Maximum length of dialed number, **5**
   - **SIP Domain:** Select -ALL-
3. Under **Originating Locations and Routing Policies**, click **Add**, and then select the appropriate location and routing policy from the list (not shown).

   Default values can be used for the remaining fields.
4. Click **Commit** to save the dial pattern.

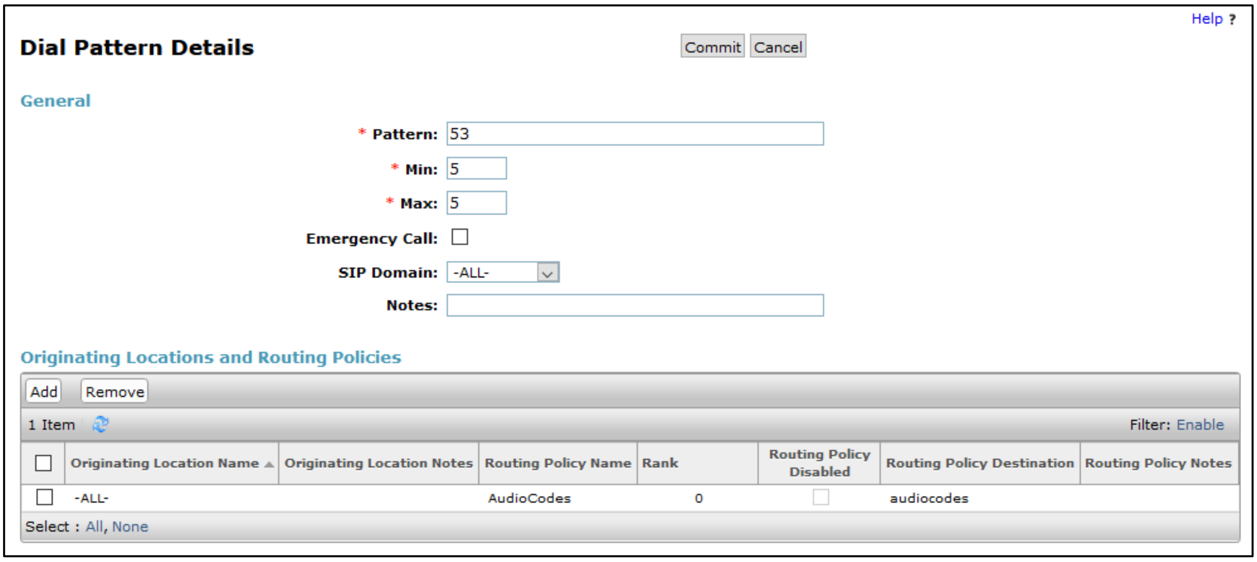
Figure 3-10: Dial Plan Details



5. Repeat the process to add one or more dial patterns for routing calls to PSTN numbers via AudioCodes Mediant SBC.
6. Fill in the following fields as specified for routing calls to AudioCodes Mediant SBC:
   - Under **General**:
     - **Pattern:** Dialed number or prefix, **53**
     - **Min:** Minimum length of dialed number, **5**
     - **Max:** Maximum length of dialed number, **5**
     - **SIP Domain:** Select -ALL-
   - Under **Originating Locations and Routing Policies**, click **Add**, and then select the appropriate location and routing policy from the list (not shown). Default values can be used for the remaining fields.

7. Click **Commit** to save the dial pattern.

Figure 3-11: Dial Plan Details



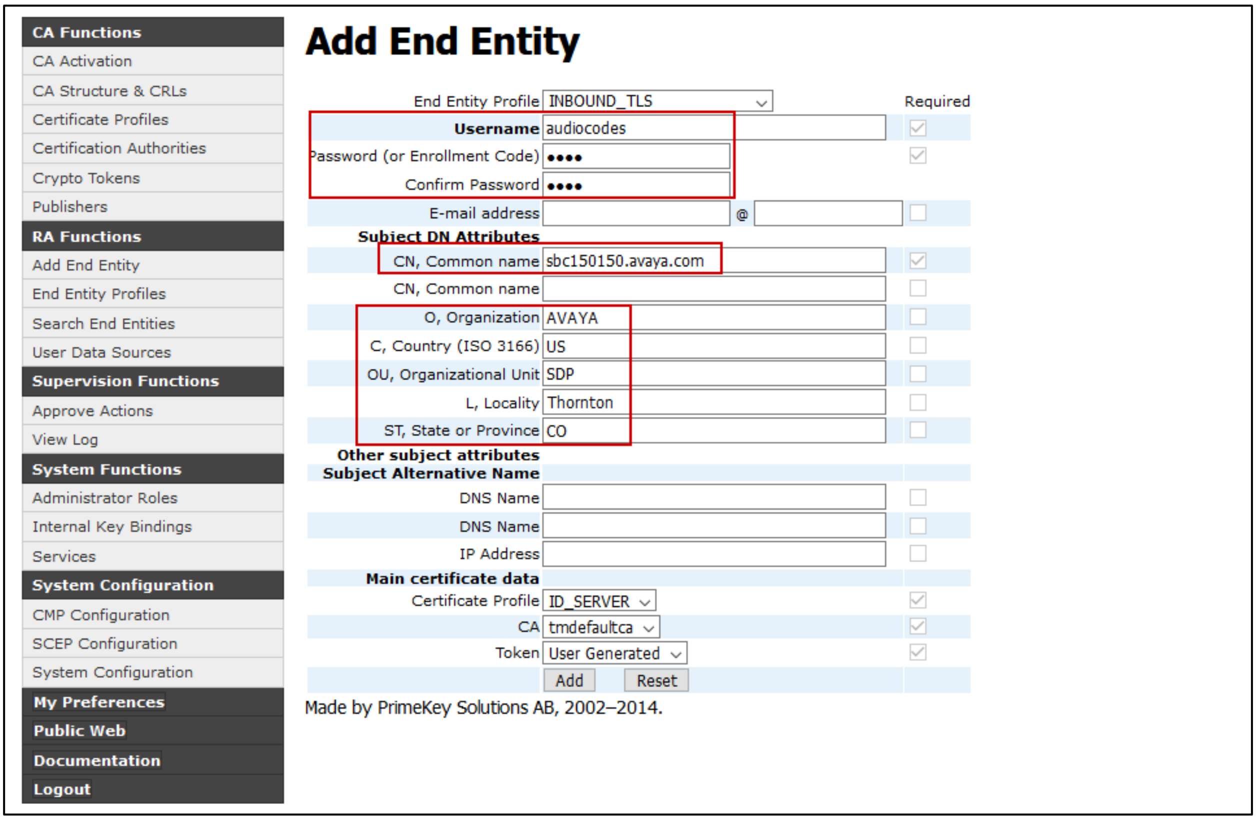
3.2.7 Generate AudioCodes Device Certificate

During the compliance test, the device certificate for AudioCodes Mediant SBC was signed by the System Manager. Once the CSR has been obtained as performed in Section 4.3.3, you can perform the procedure described below.

➢ **Do the following:**

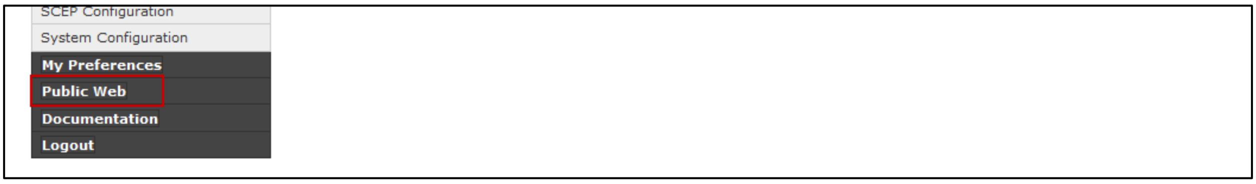
1. Navigate to **Services >Security > Certificates > Authority > Add End Entity**, and then configure the following fields:
   - **Username:** Type a username for AudioCodes entity
   - **Password:** Type in a password that will be used in Section 4.3.
   - **Confirm Password:** Re-type the password.
2. Configure the other highlighted fields as required. Retain default values for the fields that are not highlighted, and then select **Add**.

Figure 3-12: Add End Entity



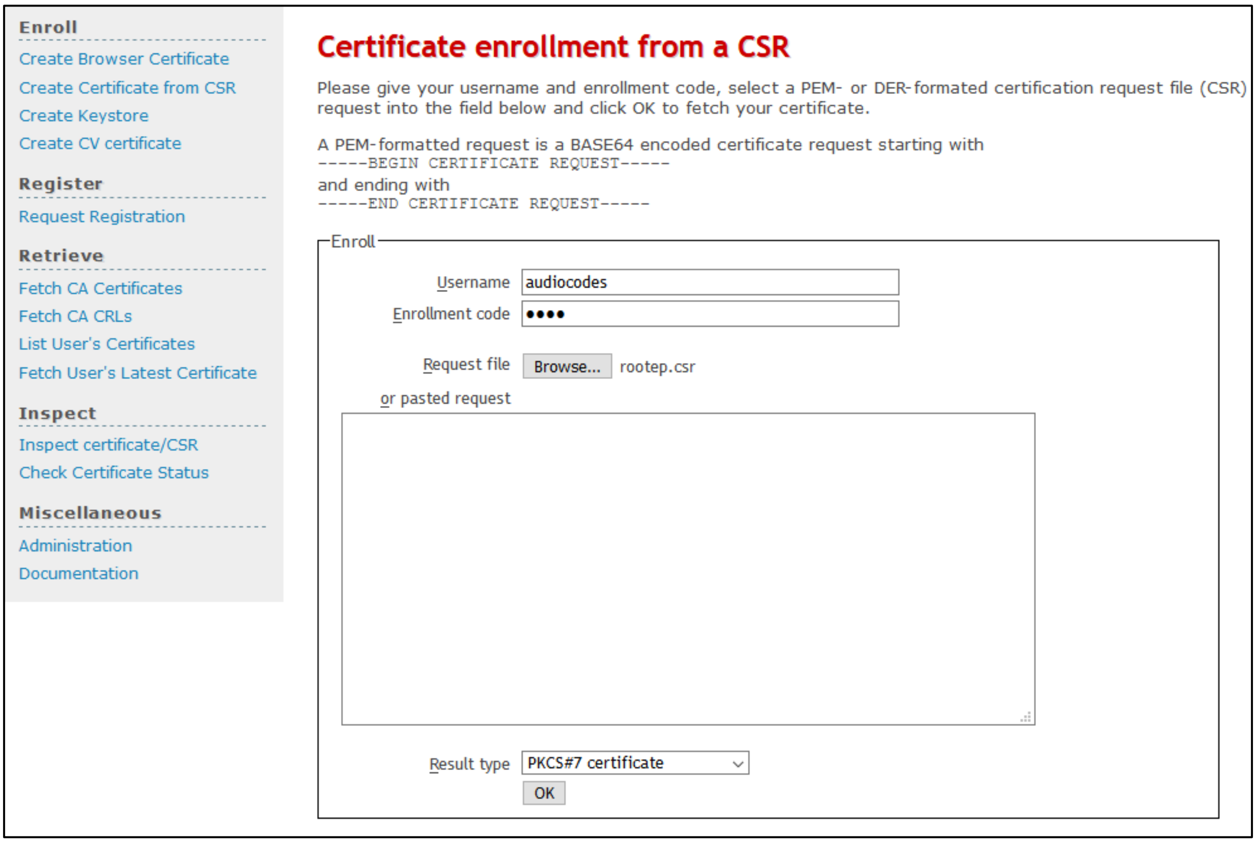
3. Once added, select **Public Web** on the left pane. Ensure that pop-up blocked is disabled as a new tab is opened in the browser.

Figure 3-13: Add Entity-Public Web



4. Select **Create Certificate from CSR** on the left. Type in the **Username** and **Password** for the newly added End Entity for **Username** and **Enrollment Code,** respectively.
5. Select the CSR obtained from the procedure described in Section 4.3.3.
6. Set **Result Type** to **PKCS#7 certificate** and select **OK.** The user will be prompted to save certificate (not shown).
7. Save the certificate, it will be later used in Section 4.3.3**.**

Figure 3-14: Certificate Enrollment form a CSR



This page is intentionally left blank.

4 Configuring AudioCodes SBC

This section provides step-by-step procedures on how to configure AudioCodes SBC for interworking between Avaya Aura Platform and the Generic SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

- SBC LAN interface – Management Station and Avaya Aura Platform
- SBC WAN interface – Generic SIP Trunking

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

Notes:

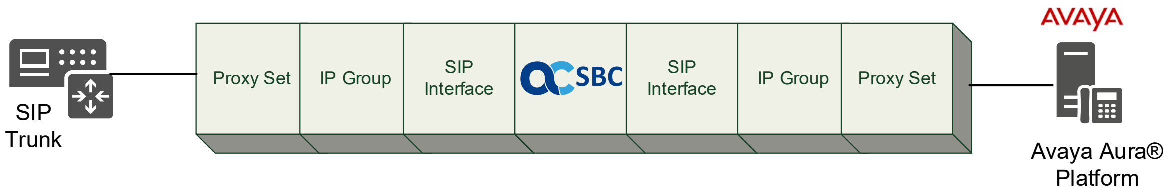
- For implementing Avaya Aura Platform and Generic SIP Trunk based on the configuration described in this section, AudioCodes SBC must be installed with a License Key that includes the following software features:
    - **Number of SBC sessions** (based on requirements)
    - **Transcoding sessions** (only if media transcoding is needed)
    - **Coders** (based on requirements)

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

4.1 SBC Configuration Concept

The diagram below represents AudioCodes' device configuration concept for this interoperability test topology.

Figure 4-1: SBC Configuration Concept

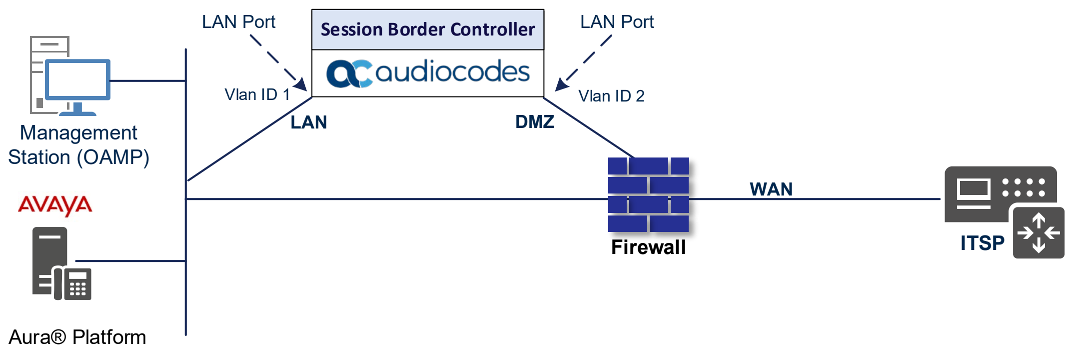


4.2 IP Network Interfaces Configuration

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

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

Figure 4-2: Network Interfaces in Interoperability Test Topology



4.2.1 Configure VLANs

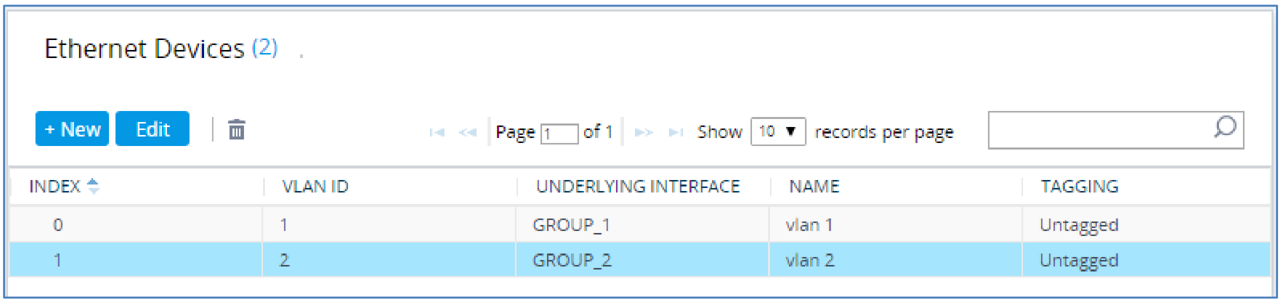
This section describes how to configure VLANs for each of the following interfaces:

- LAN VoIP (assigned the name "acsbc.avaya.com")
- WAN VoIP (assigned the name "External")

➢ **To configure the VLANs:**

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

Figure 4-3: Configured VLAN IDs in Ethernet Device



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 "acsbc.avaya.com")
- WAN Interface (assigned the name "External")

➢ **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	acsbc.avaya.com	vlan 1
1	Media + Control (as this interface points to the internet, enabling OAMP is not recommended)	IPv4 Manual	195.189.192.157 (DMZ IP address of SBC)	25	195.189.192.129 (router's IP address)	According to your Internet provider's instructions	External	vlan 2

The configured IP network interfaces are shown below:

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

IP Interfaces (2)

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

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	acsbc.avaya.com	OAMP + Media + (	IPv4 Manual	10.15.77.77	16	10.15.0.1	10.1.1.6	10.1.1.10	vlan 1
1	External	Media + Control	IPv4 Manual	195.189.192.156	24	195.189.192.129	80.179.52.100	80.179.55.100	vlan 2

4.3 SIP TLS Connection Configuration

This section describes how to configure the SBC for using a TLS connection with the Avaya Aura Platform and Generic SIP Trunk. This configuration is essential for a secure SIP TLS connection. The certificate module is based on the Service Provider's own TLS Certificate. For more certificate structure options, refer to Avaya Aura Platform documentation.

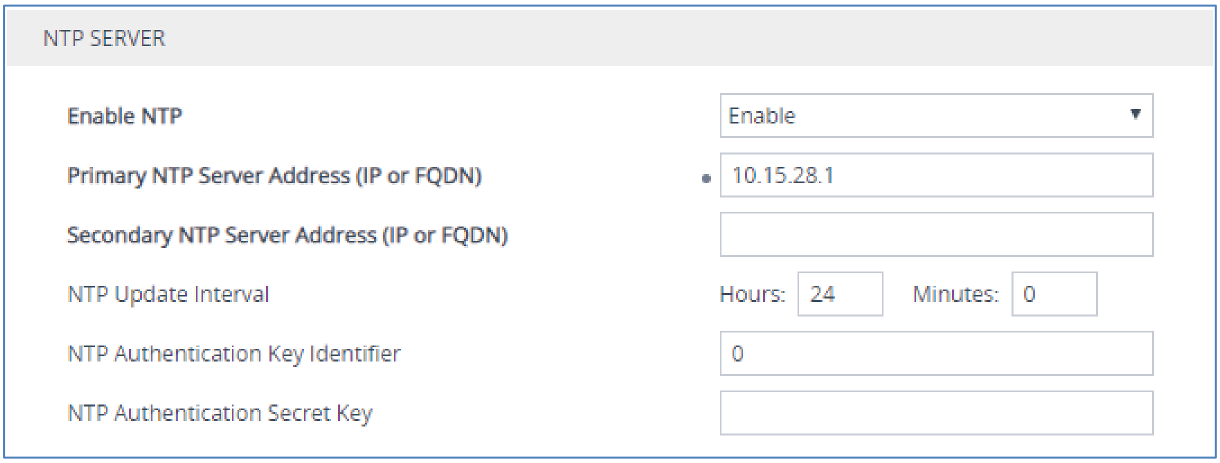
4.3.1 Configure the NTP Server Address

This section describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or another global 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 NTP server will locate on the OAMP IP Interface (acsbc.avaya.com 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 NTP server (e.g., **10.15.28.1**).

Figure 4-5: Configuring NTP Server Address



3. Click **Apply**.

4.3.2 Create a TLS Context

This section describes how to configure TLS Context in the SBC. AudioCodes recommends implementing only TLS to avoid flaws in SSL.

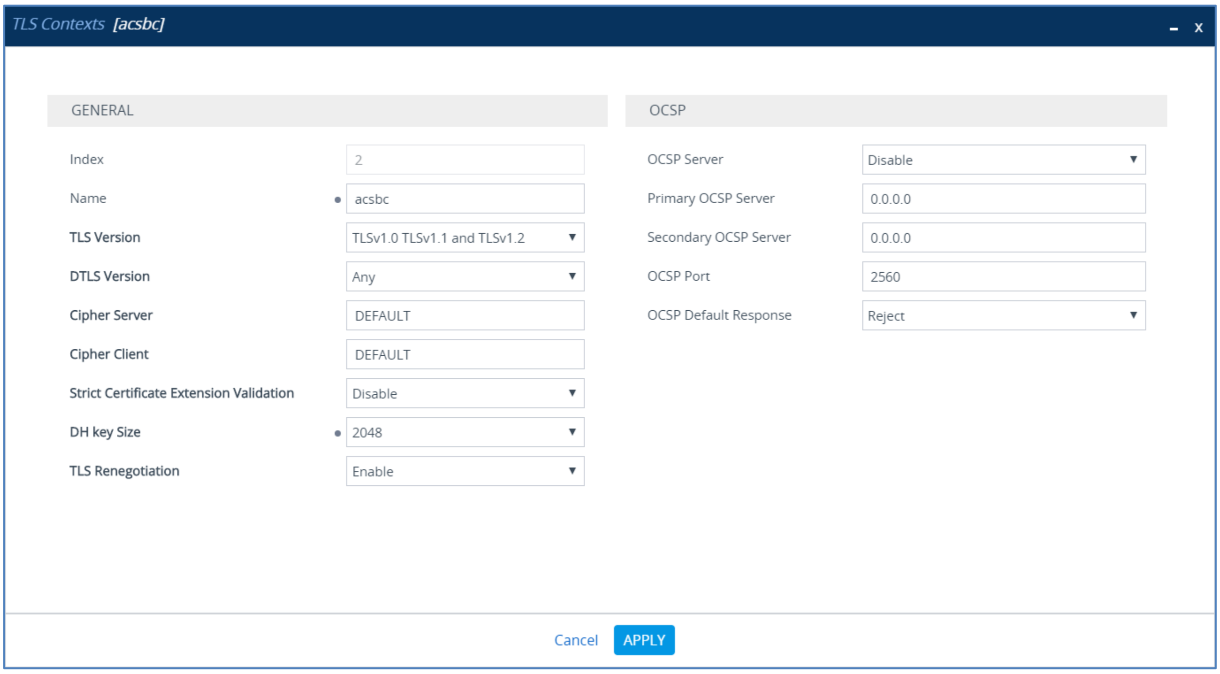
➢ **To configure the TLS version:**

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

Table 4-2: New TLS Context

Index	Name	DH key Size
1	**acsbc** (arbitrary descriptive name)	**2048**
All other parameters can be left unchanged with their default values.		

Figure 4-6: Configuring TLS Context



3. Click **Apply**.

4.3.3 Configure a Certificate

This section describes how to exchange a certificate with Avaya Certificate Authority (in our case, Avaya Aura System Manager). The certificate is used by the SBC to authenticate the connection with the Avaya Aura Platform.

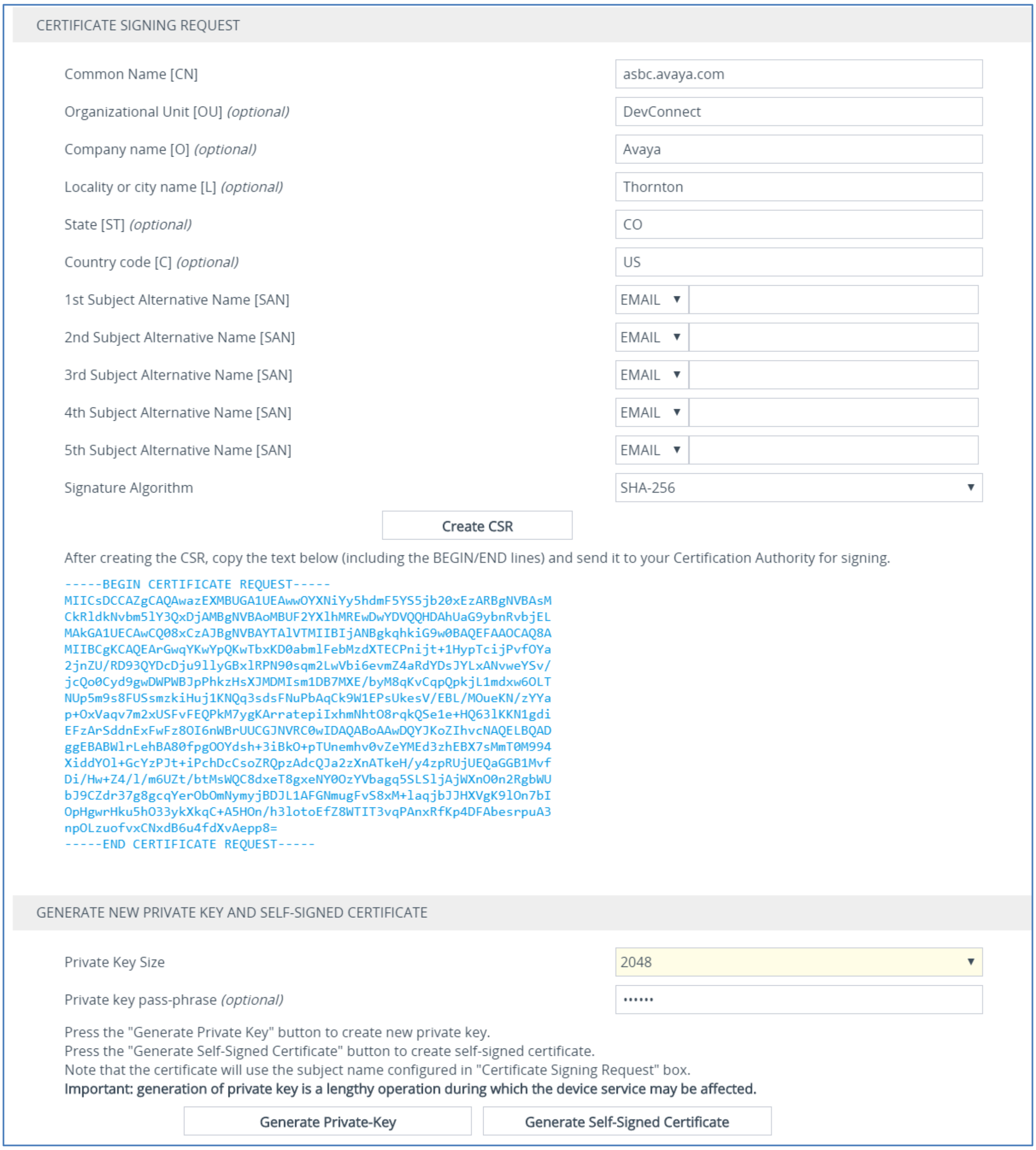
The procedure involves the following main steps:

a. Generating a Certificate Signing Request (CSR).
b. Requesting Device Certificate from CA.
c. Obtaining Trusted Root/ Intermediate Certificate from CA.
d. Deploying Device and Trusted Root/ Intermediate Certificates on SBC.

➢ **To configure a certificate:**

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the required TLS Context index row (**acsbc** in our case), 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 'Subject Name [CN]' field, enter the SBC FQDN name (based on our example, **acsc.avaya.com**).
   b. Change the 'Private Key Size' based on the requirements of your Certification Authority. Many CAs do not support private key of size 1024. In this case, you must change the key size to 2048.
   c. To change the key size on TLS Context, go to: **Generate New Private Key and Self-Signed Certificate**, change the 'Private Key Size' to **2048** and then click **Generate Private-Key**. To use **1024** as a Private Key Size value, you can click **Generate Private-Key** without changing the default key size value.
   d. Fill in the rest of the request fields according to your security provider's instructions.
   e. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure 4-7: Example of Certificate Signing Request – Creating CSR



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 the file name, for example *certreq.txt*.
5. Sign a CSR by Avaya Aura System Manager as described in Section 3.2.7.
6. 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 (**acsbc** in our case), 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 Avaya Aura System Manager to load.
7. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.

4.4 Configure Media Realms

This section describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for the SIP Trunk traffic and one for Avaya Aura Platform traffic.

➢ **To configure Media Realms:**

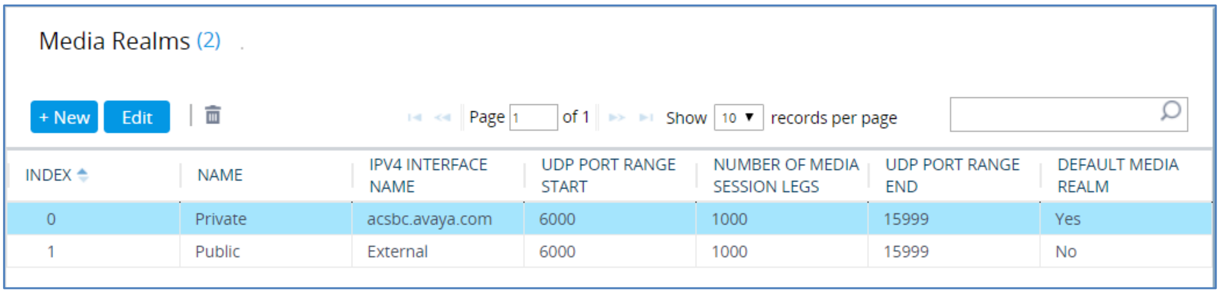
1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Configure Media Realms as follows (you can use the default Media Realm (Index 0), however modify it):

Table 4-3: Configuration Example Media Realms in Media Realm Table

Index	Name	Topology Location	IPv4 Interface Name	Port Range Start	Number of Media Session Legs
0	**Private** (arbitrary name)		acsbc.avay.com	6000	1000 (media sessions assigned with port range)
1	**Public** (arbitrary name)	Up	External	6000	1000 (media sessions assigned with port range)

The configured Media Realms are shown in the figure below:

Figure 4-8: Configured Media Realms in Media Realm Table



INDEX	NAME	IPV4 INTERFACE NAME	UDP PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	UDP PORT RANGE END	DEFAULT MEDIA REALM
0	Private	acsbc.avaya.com	6000	1000	15999	Yes
1	Public	External	6000	1000	15999	No

4.5 Configure SIP Signaling Interfaces

This section describes how to configure SIP Interfaces. For the interoperability test topology, towards the SIP Trunk and towards the Avaya Aura Platform SIP Interfaces must be configured for the SBC.

➢ **To configure SIP Interfaces:**

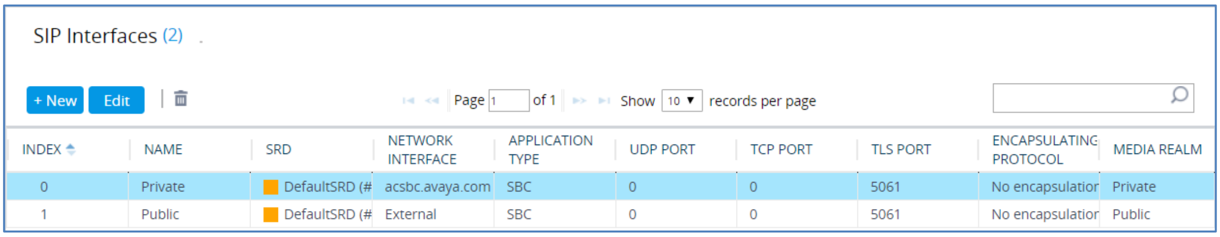
1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Configure SIP Interfaces. You can use the default SIP Interface (Index 0), but modify it as shown in the table below. The table below shows an example of the configuration.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

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

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Media Realm	TLS Context Name
0	**Private** (arbitrary name)	**acsbc.avaya.com**	**SBC**	**0**	**0**	**5061**	**Private**	**acsbc**
1	**Public** (arbitrary name)	**External**	**SBC**	**0**	**0**	**5061**	**Public**	**acsbc**

The configured SIP Interfaces are shown in the figure below:

Figure 4-9: Configured SIP Interfaces in SIP Interface Table



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:

- Generic SIP Trunk
- Avaya Session Manager

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

➢ **To configure Proxy Sets:**

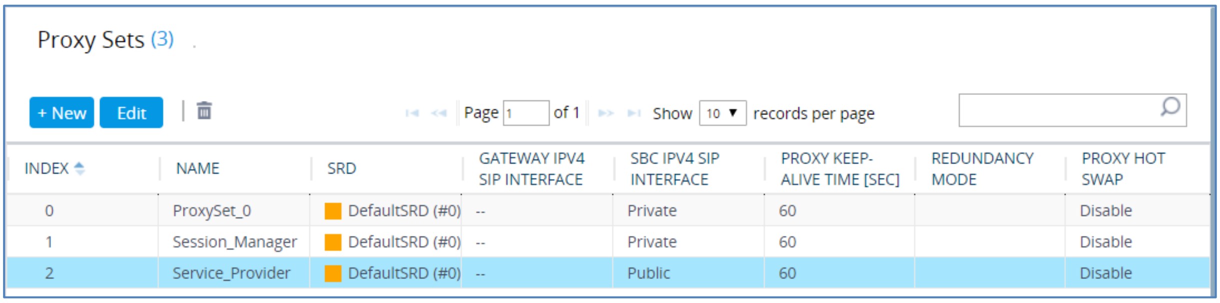
1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Configure Proxy Sets as shown in the table below:

Table 4-5: Configuration Example Proxy Sets in Proxy Sets Table

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive
1	**Session_Manager** (arbitrary name)	Private	acsbc	Using Options
2	**Service_Provider** (arbitrary name)	Public	acsbc	Using Options

The configured Proxy Sets are shown in the figure below:

Figure 4-10: Configured Proxy Sets in Proxy Sets Table



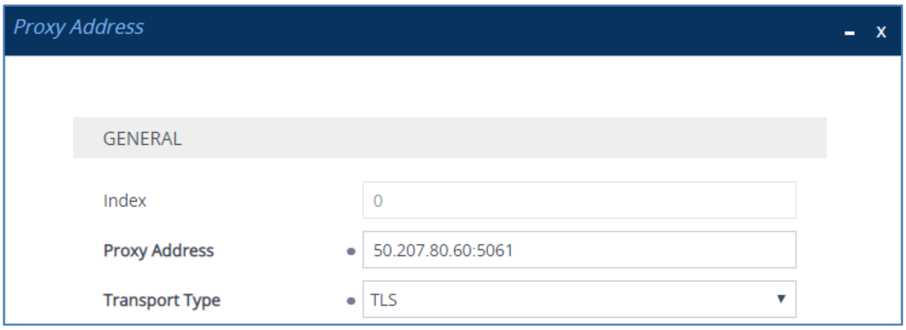
4.6.1 Configure a Proxy Address

This section shows how to configure a Proxy address.

➢ **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 **Service_Provider**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**; the following dialog box appears:

Figure 4-11: Configuring Proxy Address for SIP Trunk



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

Table 4-6: Configuration Proxy Address for SIP Trunk

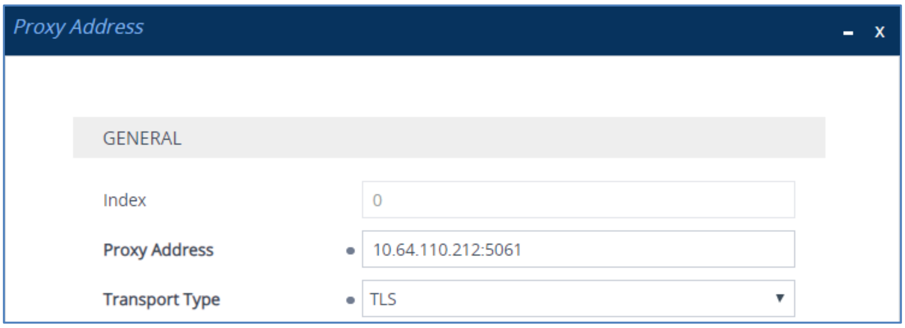
Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	50.207.80.60:5061 (SIP Trunk IP and port)	TLS	0	0

4. Click **Apply**.

➢ To configure a Proxy Address for Avaya Session Manager:

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

Figure 4-12: Configuring Proxy Address for Avaya Session Manager



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

Table 4-7: Configuration Proxy Address for Avaya Session Manager

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	10.64.110.212:5061 (Avaya Session Manager IP and port)	TLS	0	0

4. Click **Apply**.

4.7 Configure Coders

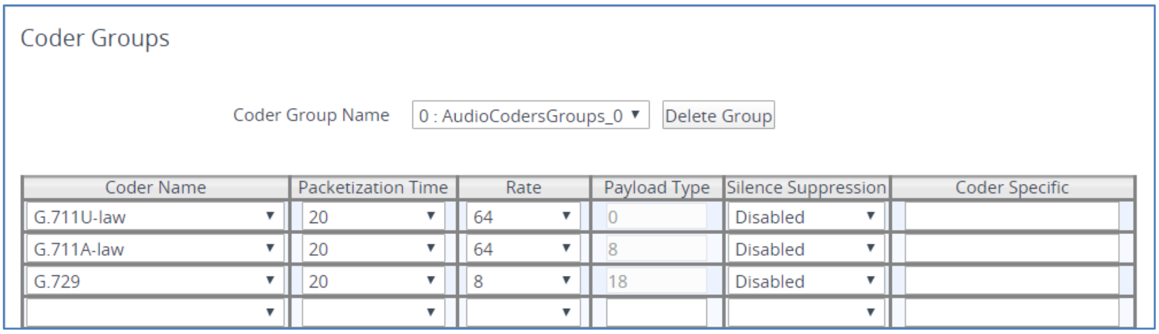
This section describes how to configure coders (termed *Coder Group*). Note that the Coder Group ID for this entity will be assigned to its corresponding IP Profile in the next step.

➢ **To configure coders:**

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

Parameter	Value
Coder Group Name	**AudioCodersGroups_0**
Coder Name	▪ **G.711 U-law** ▪ **G.711 A-law** ▪ **G.729**

Figure 4-13: Configuring Default Coder Group



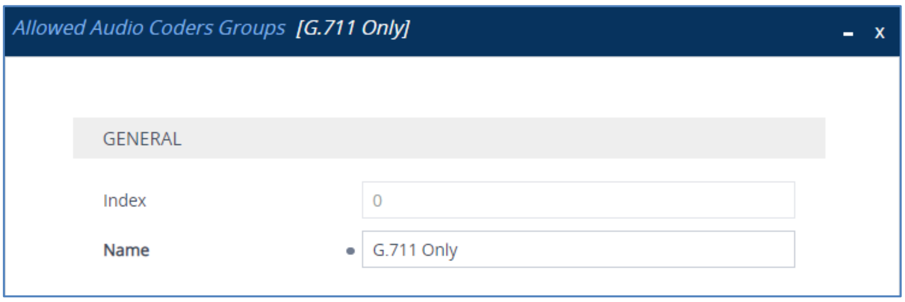
3. Click **Apply,** and then confirm the configuration change in the prompt that pops up.

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the Generic SIP Trunk and Avaya Aura Platform uses the dedicated coders list whenever possible. Note that this Allowed Coders Group ID will be assigned to the appropriated IP Profiles in the next step.

➢ **To set the allowed coders:**

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 Generic SIP Trunk.

Figure 4-14: Configuring Allowed Coders Group

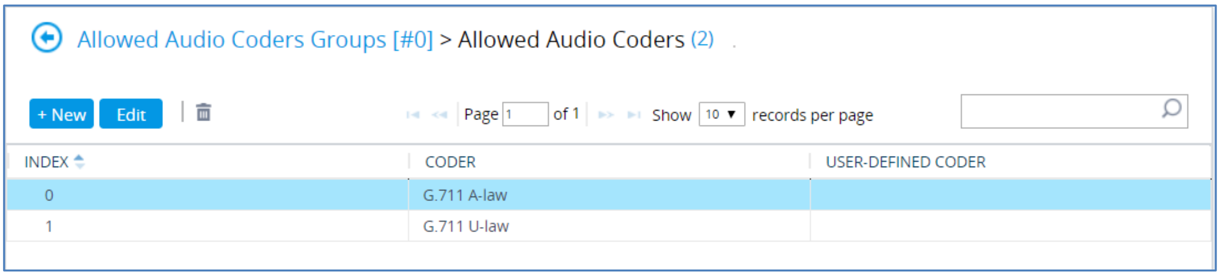


3. Click **Apply**.

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 A-law
1	G.711 U-law

Figure 4-15: Configuring Allowed Coders



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).

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

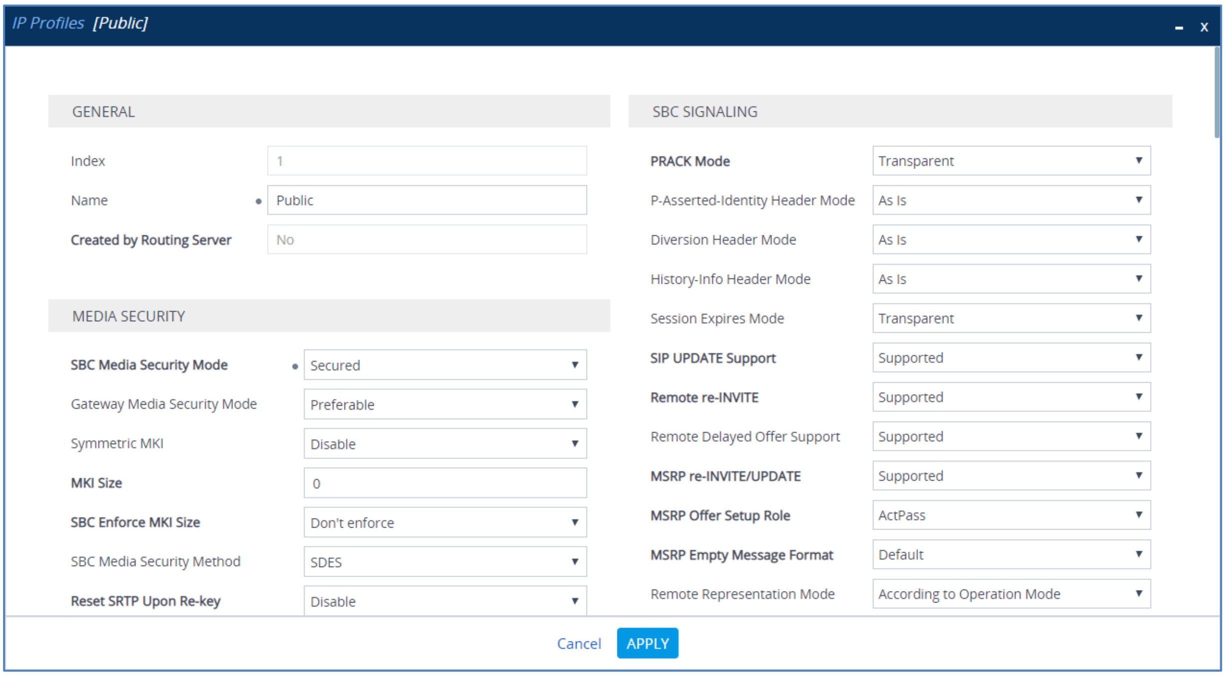
- Generic SIP trunk – to operate in secure mode using SRTP and SIP over TLS
- Avaya Aura Platform – to operate in secure mode using SRTP and SIP over TLS

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

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

Parameter	Value
General	
Index	**1**
Name	**Public**
Media Security	
SBC Media Security Mode	**Secured**
SBC Media	
Allowed Audio Coders	**G.711 Only**
Allowed Coders Mode	**Preference** (lists Allowed Coders first and then original coders in received SDP offer)

Figure 4-16: Configuring IP Profile for Generic SIP Trunk



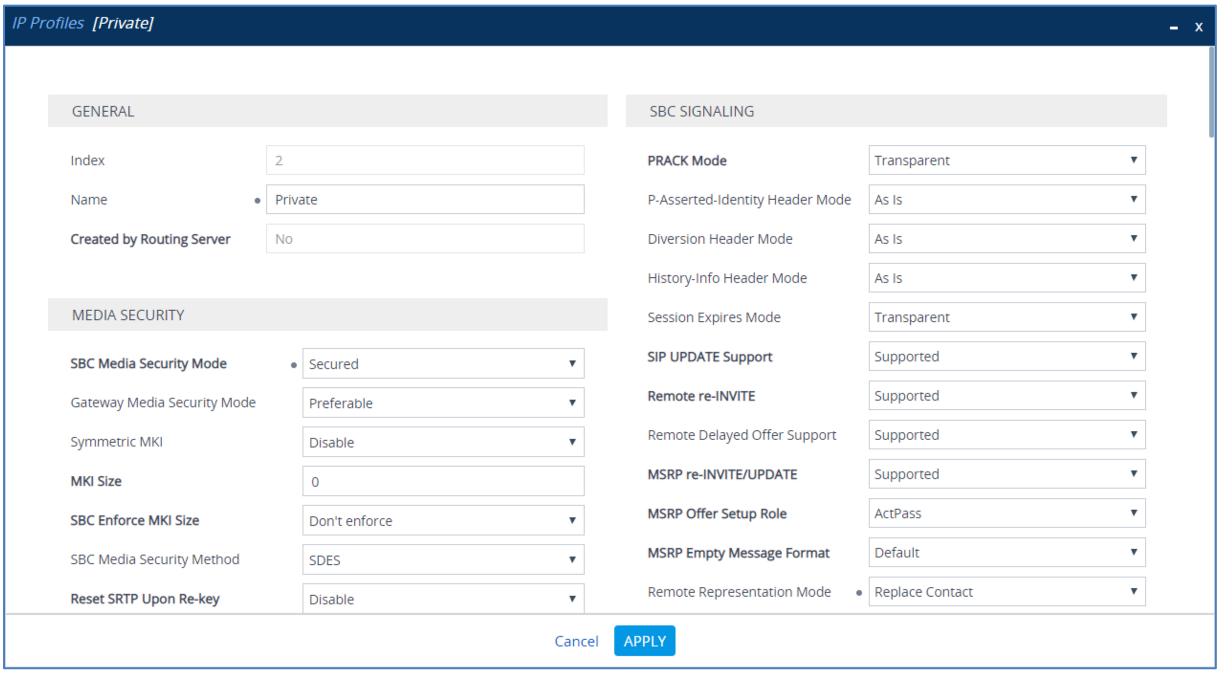
3. Click **Apply**.

➢ To configure IP Profile for Avaya Aura platform :

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

Parameter	Value
General	
Index	**2**
Name	**Private** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**Secured**
SBC Media	
Allowed Audio Coders	**G.711 Only**
Allowed Coders Mode	**Preference** (lists Allowed Coders first and then original coders in received SDP offer)
SBC Signaling	
Remote Representation Mode	**Replace Contact**

Figure 4-17: Configuring IP Profile for Avaya Aura Platform



3. Click **Apply**.

4.9 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:

- Generic SIP Trunk located on WAN
- Avaya Aura Platform located on LAN

➢ **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 Avaya Aura platform:

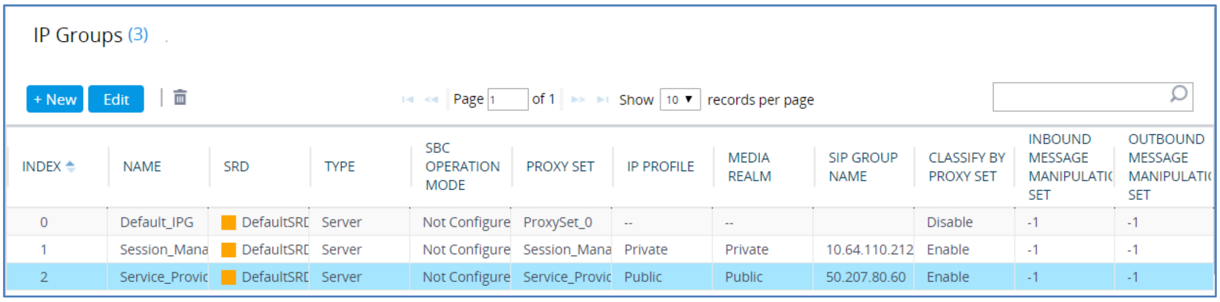
Parameter	Value
Index	**1**
Name	**Session_Manager**
Type	**Server**
Proxy Set	**Session_Manager**
IP Profile	**Private**
Media Realm	**Private**
SIP Group Name	(according to ITSP requirement)

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

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

The configured IP Groups are shown in the figure below:

Figure 4-18: Configured IP Groups in IP Group Table



INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATIC SET	OUTBOUND MESSAGE MANIPULATIC SET
0	Default_IPG	DefaultSRI	Server	Not Configure	ProxySet_0	--	--		Disable	-1	-1
1	Session_Mana	DefaultSRI	Server	Not Configure	Session_Mana	Private	Private	10.64.110.212	Enable	-1	-1
2	Service_Provic	DefaultSRI	Server	Not Configure	Service_Provic	Public	Public	50.207.80.60	Enable	-1	-1

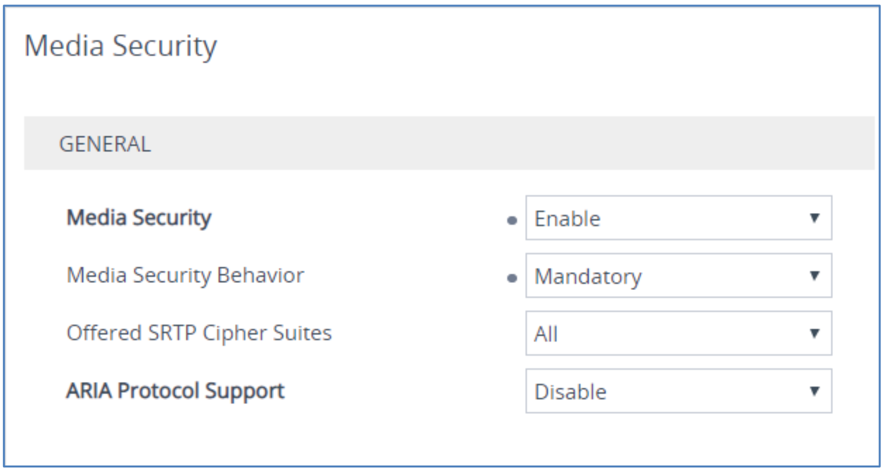
4.10 Configure Media Security

This section describes how to configure media security. The Avaya Aura Platform requires the implementation of SRTP, therefore you need to configure the SBC to operate in the same manner.

➢ **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. From the 'Media Security Behavior' drop-down list, select **Mandatory**.

Figure 4-19: Configuring SRTP



4. Click **Apply**.

4.11 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 Avaya Aura Platform and Generic SIP Trunk:

- Terminate SIP OPTIONS messages on the SBC that are received from any entity
- Calls from Avaya Aura Platform to Generic SIP Trunk
- Calls from Generic SIP Trunk to Avaya Aura Platform

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

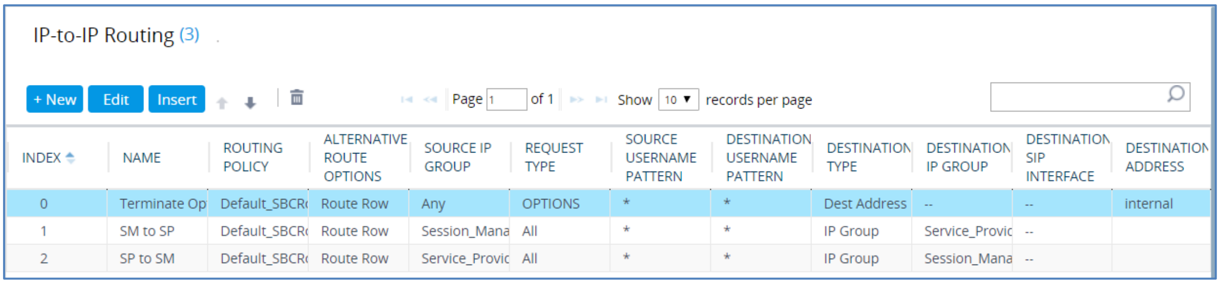
1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Configure routing rules as shown in the table below:

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

Index	Name	Source IP Group	Request Type	Dest Type	Dest IP Group	Dest Address
0	Terminate Options	Any	OPTIONS	Dest Address		internal
1	SM to SP (arbitrary name)	Session_Manager		IP Group	Service_Provider	
2	SP to SM (arbitrary name)	Service_Provider		IP Group	Session_Manager	

The configured routing rules are shown in the figure below:

Figure 4-20: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table



INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	Terminate Op	Default_SBCR	Route Row	Any	OPTIONS	*	*	Dest Address	--	--	internal
1	SM to SP	Default_SBCR	Route Row	Session_Mana	All	*	*	IP Group	Service_Provic	--	
2	SP to SM	Default_SBCR	Route Row	Service_Provic	All	*	*	IP Group	Session_Mana	--	

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

4.12 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

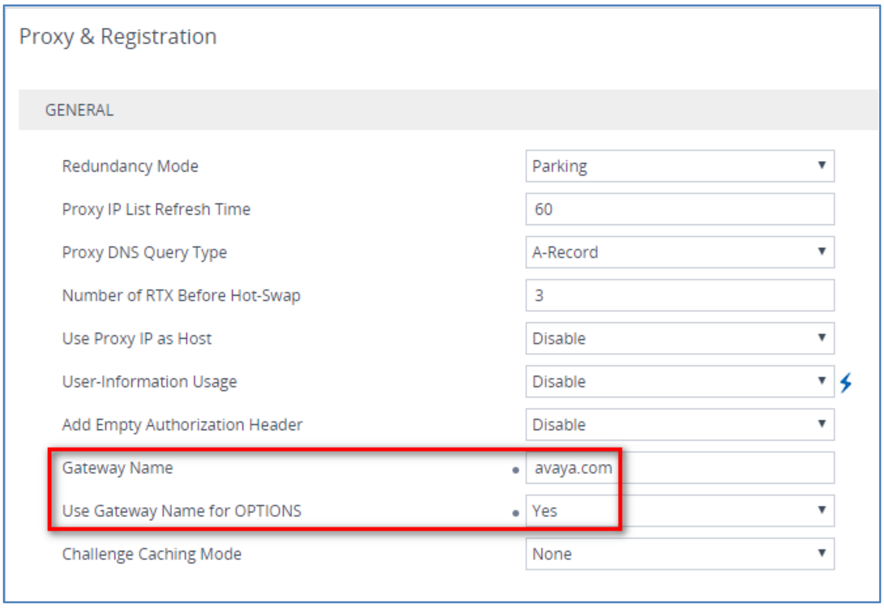
4.12.1 Configure SBC to send Domain Name in SIP OPTIONS Request

This section describes how to configure the SBC to send Domain Name in SIP OPTIONS Request messages. For the interoperability test topology, it's necessary to send Domain Name in Request URI of SIP OPTIONS keep-alive messages. This step shows how to configure the SBC to do this.

➢ **To configure Domain Name in OPTIONS:**

1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Proxy & Registration**).
2. Configure the 'Gateway Name' parameter with appropriated information (For example, **avaya.com**)
3. From the 'Use Gateway Name for OPTIONS' drop-down list, select **Yes**.

Figure 4-21: Configuring Domain Name in SIP OPTIONS



4. Click **Apply**.

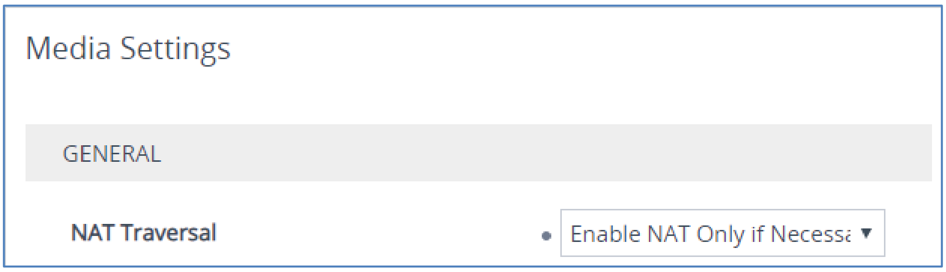
4.12.2 Configure SBC to Enforce Media Order and define NAT Mode

This section describes how to configure the SBC to Enforce Media Order according to RFC 3264 and define NAT Traversal mode.

➢ **To configure SBC to enforce media order and define NAT traversal mode:**

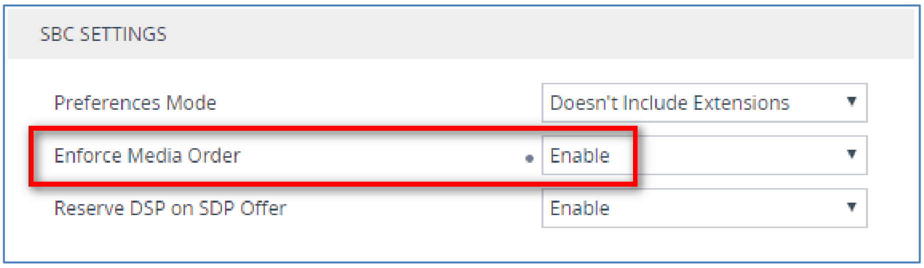
1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Settings**).
2. From the 'NAT Traversal' in the General settings area drop-down list, select **Enable NAT Only if Necessary**.

Figure 4-22: Configuring NAT Traversal Mode



3. From the 'Enforce Media Order' in the SBC settings area drop-down list, select **Enable**.

Figure 4-23: Configuring Enforce Media Order



4. Click **Apply**.

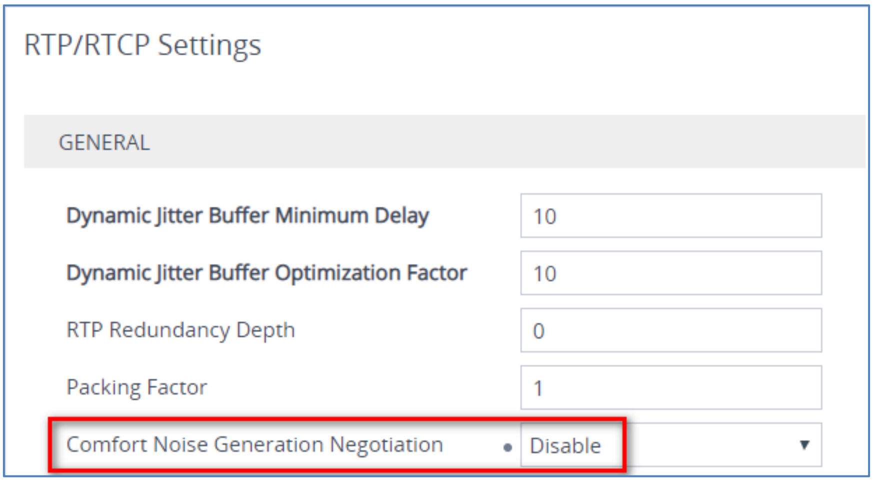
4.12.3 Disable Comfort Noise Negotiation

This section describes how to configure the SBC to disable comfort noise negotiation.

➢ **To configure SBC to disable comfort noise negotiation:**

1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **RTP/RTCP Settings**).
2. From the 'Comfort Noise Generation Negotiation' drop-down list, select **Disable**.

Figure 4-24: Disable Comfort Noise Negotiation



3. Click **Apply**.

4.12.4 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 this profile. The supported profiles include:

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

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

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

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

This page is intentionally left blank.

A AudioCodes INI File

The *ini* configuration file of the SBC, corresponding to the Web-based configuration as described in Section 4 on page 31, is shown below:

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

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

;Time & Date: 13/02/2020 16:18:23
;Device Up Time: 16d:17h:21m:43s
;Board: Mediant SW
;Board Type: 73
;Serial Number: 235293687373597
;Software Version: 7.20A.256.024
;ISO Version: 7.20A.254.202
;DSP Software Version: SOFTDSP => 0.00
;Board IP Address: 10.64.110.82
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 10.64.110.1
;Virtual Env.: vmware
;CPU: Intel(R) Xeon(R) CPU X5670@2.93GHz, total 1 cores, 1 cpus, 1
sockets, HT disabled, avx not supported
;Cores mapping:
;core #0, on cpu #0, on socket #0
;Memory: 4096 MB
;Disk total size: 3936 MB, Disk free space: 3924 MB, Disk used space: <
1%
;Network:
;      VMware VMXNET3 Ethernet Controller (rev 01)
;      VMware VMXNET3 Ethernet Controller (rev 01)

;Virtual Network: None
;Num of DSP Cores: 0
;;;Key features:;Board Type: Mediant SW ;Max SW Ver: 9.80;Coders: G723
G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB
G722 EG711 MS_RTA_NB MS_RTA_WB SILK_NB SILK_WB SPEEX_NB SPEEX_WB OPUS_NB
OPUS_WB EVS ;DSP Voice features: ;Security: MediaEncryption
StrongEncryption EncryptControlProtocol ;Channel Type: DspCh=0 ;HA ;QOE
features: VoiceQualityMonitoring MediaEnhancement ;Control Protocols:
MSFT FEU=3 SIPRec=3 CODER-TRANSCODING=3 EMS WebRTC=-1 TEAMS MGCP SIP
SBC=3 ;Default features:;Coders: G711 G726;


;MAC Addresses in use:
;---------------------------
;GROUP_1 - 00:50:56:ab:d4:d6 - vmxnet3
;GROUP_2 - 00:50:56:ab:7f:c9 - vmxnet3
;----------------------------------------------

;----------------------------------------------
```

```
[SYSTEM Params]

SyslogServerIP = 10.64.10.47
EnableSyslog = 1
ENABLEPARAMETERSMONITORING = 1
ActivityListToLog = 'pvc', 'afl', 'dr', 'fb', 'swu', 'naa', 'spc', 'll',
'cli', 'ae'
TLSPkeySize = 2048
HALocalMAC = '005056abd4d6'
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
NTPServerIP = '0.0.0.0'

[BSP Params]

PCMLawSelect = 3
ARPTableMaxEntries = 3408
UdpPortSpacing = 4
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95
SbcPerformanceProfile = 0

[ControlProtocols Params]


[Voice Engine Params]

NatMode = 0
RTCPEncryptionDisableTx = 1
ENABLEMEDIASECURITY = 1
SbcClusterMode = 0
SbcDeviceRole = 0
PLThresholdLevelsPerMille_0 = 5
PLThresholdLevelsPerMille_1 = 10
PLThresholdLevelsPerMille_2 = 20
PLThresholdLevelsPerMille_3 = 50

[WEB Params]

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

[SIP Params]

GWDEBUGLEVEL = 5
SIPGATEWAYNAME = 'avaya.com'
USEGATEWAYNAMEFOROPTIONS = 1
MEDIASECURITYBEHAVIOUR = 1
COMFORTNOISENEGOTIATION = 0
MSLDAPPRIMARYKEY = 'telephoneNumber'
SBCENFORCEMEDIAORDER = 1
ENERGYDETECTORCMD = 104
ANSWERDETECTORCMD = 12582952

[SNMP Params]
```

```
SNMPManagerTableIP = ::
SNMPTRUSTEDMGR = ::

[ PhysicalPortsTable ]

FORMAT Index = Port, Mode, SpeedDuplex, PortDescription, GroupMember;
PhysicalPortsTable 0 = "GE_1", 1, 4, "User Port #0", "GROUP_1";
PhysicalPortsTable 1 = "GE_2", 1, 4, "User Port #1", "GROUP_2";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT Index = Group, Mode, Member1, Member2;
EtherGroupTable 0 = "GROUP_1", 1, "GE_1", "";
EtherGroupTable 1 = "GROUP_2", 1, "GE_2", "";
EtherGroupTable 2 = "GROUP_3", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";
EtherGroupTable 4 = "GROUP_5", 0, "", "";
EtherGroupTable 5 = "GROUP_6", 0, "", "";
EtherGroupTable 6 = "GROUP_7", 0, "", "";
EtherGroupTable 7 = "GROUP_8", 0, "", "";
EtherGroupTable 8 = "GROUP_9", 0, "", "";
EtherGroupTable 9 = "GROUP_10", 0, "", "";
EtherGroupTable 10 = "GROUP_11", 0, "", "";
EtherGroupTable 11 = "GROUP_12", 0, "", "";
EtherGroupTable 12 = "GROUP_13", 0, "", "";
EtherGroupTable 13 = "GROUP_14", 0, "", "";
EtherGroupTable 14 = "GROUP_15", 0, "", "";

[ \EtherGroupTable ]


[ DeviceTable ]

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

[ \DeviceTable ]


[ InterfaceTable ]

FORMAT Index = ApplicationTypes, InterfaceMode, IPAddress, PrefixLength,
Gateway, InterfaceName, PrimaryDNSServerIPAddress,
SecondaryDNSServerIPAddress, UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.64.110.82, 24, 10.64.110.1,
"acsbc.avaya.com", 10.64.110.100, 75.75.75.75, "vlan 1";
InterfaceTable 1 = 5, 10, 50.207.80.26, 25, 50.207.80.1, "External",
0.0.0.0, 0.0.0.0, "vlan 2";

[ \InterfaceTable ]
```

```
[ WebUsers ]

FORMAT Index = Username, Password, Status, PwAgeInterval, SessionLimit, CliSessionLimit, SessionTimeout, BlockTime, UserLevel, PwNonce, SSHPublicKey;
WebUsers 0 = "Admin", "$1$grPhtOPk5u7vvOjvvLy/8qTx96Sip6L9qP+tqqSprMGWlpWQlcfBmZvInJXMzMyDgdSFgIfQj9uAid6Ij9jcovY=", 1, 0, 5, -1, 15, 60, 200, "08c7a82bd928f9ea00192c53cac0aeb3", "";
WebUsers 1 = "User", "$1$nfmpqMLFl5uRl5SRzZCTmcnJz56G0ouG19SO1ImB2Y+KidrZpfWk9fCj//6q8aut+/X8reLotOq17O/lveDov74=", 1, 0, 5, -1, 15, 60, 50, "bbebaf6abf2df8578bd7c8397da2d86f", "";

[ \WebUsers ]


[ TLSContexts ]

FORMAT Index = Name, TLSVersion, DTLSVersion, ServerCipherString, ClientCipherString, RequireStrictCert, TlsRenegotiation, OcspEnable, OcspServerPrimary, OcspServerSecondary, OcspServerPort, OcspDefaultResponse, DHKeySize;
TLSContexts 0 = "default", 7, 0, "DEFAULT", "DEFAULT", 0, 1, 0, 0.0.0.0, 0.0.0.0, 2560, 0, 1024;
TLSContexts 1 = "acsbc", 7, 0, "DEFAULT", "DEFAULT", 0, 1, 0, 0.0.0.0, 0.0.0.0, 2560, 0, 2048;

[ \TLSContexts ]


[ AudioCodersGroups ]

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

[ \AudioCodersGroups ]


[ AllowedAudioCodersGroups ]

FORMAT Index = Name;
AllowedAudioCodersGroups 0 = "G.711 Only";

[ \AllowedAudioCodersGroups ]


[ IpProfile ]

FORMAT Index = ProfileName, IpPreference, CodersGroupName, IsFaxUsed, JitterBufMinDelay, JitterBufOptFactor, IPDiffServ, SigIPDiffServ, RTPRedundancyDepth, CNGmode, VxxTransportType, NSEMode, IsDTMFUsed, PlayRBTone2IP, EnableEarlyMedia, ProgressIndicator2IP, EnableEchoCanceller, CopyDest2RedirectNumber, MediaSecurityBehaviour, CallLimit, DisconnectOnBrokenConnection, FirstTxDtmfOption, SecondTxDtmfOption, RxDTMFOption, EnableHold, InputGain, VoiceVolume, AddIEInSetup, SBCExtensionCodersGroupName, MediaIPVersionPreference, TranscodingMode, SBCAllowedMediaTypes, SBCAllowedAudioCodersGroupName, SBCAllowedVideoCodersGroupName, SBCAllowedCodersMode, SBCMediaSecurityBehaviour, SBCRFC2833Behavior, SBCAlternativeDTMFMethod,
```

```
SBCSendMultipleDTMFMethods, SBCAssertIdentity,
AMDSensitivityParameterSuit, AMDSensitivityLevel, AMDMaxGreetingTime,
AMDMaxPostSilenceGreetingTime, SBCDiversionMode, SBCHistoryInfoMode,
EnableQSIGTunneling, SBCFaxCodersGroupName, SBCFaxBehavior,
SBCFaxOfferMode, SBCFaxAnswerMode, SbcPrackMode, SBCSessionExpiresMode,
SBCRemoteUpdateSupport, SBCRemoteReinviteSupport,
SBCRemoteDelayedOfferSupport, SBCRemoteReferBehavior,
SBCRemote3xxBehavior, SBCRemoteMultiple18xSupport,
SBCRemoteEarlyMediaResponseType, SBCRemoteEarlyMediaSupport,
EnableSymmetricMKI, MKISize, SBCEnforceMKISize, SBCRemoteEarlyMediaRTP,
SBCRemoteSupportsRFC3960, SBCRemoteCanPlayRingback, EnableEarly183,
EarlyAnswerTimeout, SBC2833DTMFPayloadType, SBCUserRegistrationTime,
ResetSRTPStateUponRekey, AmdMode, SBCReliableHeldToneSource,
GenerateSRTPKeys, SBCPlayHeldTone, SBCRemoteHoldFormat,
SBCRemoteReplacesBehavior, SBCSDPPtimeAnswer, SBCPreferredPTime,
SBCUseSilenceSupp, SBCRTPRedundancyBehavior, SBCPlayRBTToTransferee,
SBCRTCPMode, SBCJitterCompensation, SBCRemoteRenegotiateOnFaxDetection,
JitterBufMaxDelay, SBCUserBehindUdpNATRegistrationTime,
SBCUserBehindTcpNATRegistrationTime, SBCSDPHandleRTCPAttribute,
SBCRemoveCryptoLifetimeInSDP, SBCIceMode, SBCRTCPMux,
SBCMediaSecurityMethod, SBCHandleXDetect, SBCRTCPFeedback,
SBCRemoteRepresentationMode, SBCKeepVIAHeaders, SBCKeepRoutingHeaders,
SBCKeepUserAgentHeader, SBCRemoteMultipleEarlyDialogs,
SBCRemoteMultipleAnswersMode, SBCDirectMediaTag,
SBCAdaptRFC2833BWToVoiceCoderBW, CreatedByRoutingServer,
SBCFaxReroutingMode, SBCMaxCallDuration, SBCGenerateRTP,
SBCISUPBodyHandling, SBCISUPVariant, SBCVoiceQualityEnhancement,
SBCMaxOpusBW, SBCEnhancedPlc, LocalRingbackTone, LocalHeldTone,
SBCGenerateNoOp, SBCRemoveUnKnownCrypto, SBCMultipleCoders, DataDiffServ,
SBCMSRPReinviteUpdateSupport, SBCMSRPOfferSetupRole, SBCMSRPEmpMsg;
IpProfile 1 = "Public", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0,
0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", "", 0, 0,
"", "G.711 Only", "", 1, 1, 0, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, "", 0,
0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0,
-1, -1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, -1, 0, 0, 0,
0, 1, 2, 0;
IpProfile 2 = "Private", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0,
0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", "", 0, 0,
"", "G.711 Only", "", 1, 1, 0, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, "", 0,
0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0,
0, -1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, -1, 0, 0, 0,
0, 1, 2, 0;

[ \IpProfile ]


[ CpMediaRealm ]

FORMAT Index = MediaRealmName, IPv4IF, IPv6IF, RemoteIPv4IF,
RemoteIPv6IF, PortRangeStart, MediaSessionLeg, PortRangeEnd,
TCPPortRangeStart, TCPPortRangeEnd, IsDefault, QoeProfile, BWProfile,
TopologyLocation;
CpMediaRealm 0 = "Private", "acsbc.avaya.com", "", "", "", 6000, 14883,
65531, 0, 0, 1, "", "", 0;
CpMediaRealm 1 = "Public", "External", "", "", "", 6000, 14883, 65531, 0,
0, 0, "", "", 1;

[ \CpMediaRealm ]


[ SBCRoutingPolicy ]
```

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

[ \SBCRoutingPolicy ]


[ SRD ]

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

[ \SRD ]


[ MessagePolicy ]

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

[ \MessagePolicy ]


[ SIPInterface ]

FORMAT Index = InterfaceName, NetworkInterface,
SCTPSecondaryNetworkInterface, ApplicationType, UDPPort, TCPPort,
TLSPort, SCTPPort, AdditionalUDPPorts, AdditionalUDPPortsMode, SRDName,
MessagePolicyName, TLSContext, TLSMutualAuthentication,
TCPKeepaliveEnable, ClassificationFailureResponseType,
PreClassificationManSet, EncapsulatingProtocol, MediaRealm,
SBCDirectMedia, BlockUnRegUsers, MaxNumOfRegUsers,
EnableUnAuthenticatedRegistrations, UsedByRoutingServer,
TopologyLocation, PreParsingManSetName, AdmissionProfile,
CallSetupRulesSetId;
SIPInterface 0 = "Private", "acsbc.avaya.com", "", 2, 5060, 5060, 5061,
0, "", 0, "DefaultSRD", "", "acsbc", -1, 0, 500, -1, 0, "Private", 0, -1,
-1, -1, 0, 0, "", "", -1;
SIPInterface 1 = "Public", "External", "", 2, 5060, 5060, 5061, 0, "", 0,
"DefaultSRD", "", "acsbc", -1, 0, 500, -1, 0, "Public", 0, -1, -1, -1, 0,
1, "", "", -1;

[ \SIPInterface ]


[ ProxySet ]

FORMAT Index = ProxyName, EnableProxyKeepAlive, ProxyKeepAliveTime,
ProxyLoadBalancingMethod, IsProxyHotSwap, SRDName, ClassificationInput,
TLSContextName, ProxyRedundancyMode, DNSResolveMethod,
KeepAliveFailureResp, GWIPv4SIPInterfaceName, SBCIPv4SIPInterfaceName,
GWIPv6SIPInterfaceName, SBCIPv6SIPInterfaceName, MinActiveServersLB,
SuccessDetectionRetries, SuccessDetectionInterval,
FailureDetectionRetransmissions;
```

```
ProxySet 0 = "Session_Manager", 1, 60, 0, 0, "DefaultSRD", 0, "acsbc", -
1, -1, "", "", "Private", "", "", 1, 1, 10, -1;
ProxySet 1 = "Service_Provider", 1, 60, 0, 0, "DefaultSRD", 0, "acsbc", -
1, -1, "", "", "Public", "", "", 1, 1, 10, -1;

[ \ProxySet ]


[ IPGroup ]

FORMAT Index = Type, Name, ProxySetName, VoiceAIConnector, SIPGroupName,
ContactUser, SipReRoutingMode, AlwaysUseRouteTable, SRDName, MediaRealm,
InternalMediaRealm, ClassifyByProxySet, ProfileName, MaxNumOfRegUsers,
InboundManSet, OutboundManSet, RegistrationMode, AuthenticationMode,
MethodList, SBCServerAuthType, OAuthHTTPService, EnableSBCClientForking,
SourceUriInput, DestUriInput, ContactName, Username, Password, UUIFormat,
QOEProfile, BWProfile, AlwaysUseSourceAddr, MsgManUserDef1,
MsgManUserDef2, SIPConnect, SBCPSAPMode, DTLSContext,
CreatedByRoutingServer, UsedByRoutingServer, SBCOperationMode,
SBCRouteUsingRequestURIPort, SBCKeepOriginalCallID, TopologyLocation,
SBCDialPlanName, CallSetupRulesSetId, Tags, SBCUserStickiness,
UserUDPPortAssignment, AdmissionProfile, ProxyKeepAliveUsingIPG,
SBCAltRouteReasonsSetName, TeamsMediaOptimization,
TeamsMOInitialBehavior, SIPSourceHostName;
IPGroup 0 = 0, "Session_Manager", "Session_Manager", "", "10.64.110.212",
"", -1, 0, "DefaultSRD", "Private", "", 1, "Private", -1, -1, -1, 0, 0,
"", -1, "", 0, -1, -1, "", "Admin", "$1$aCkNBwIC", 0, "", "", 0, "", "",
0, 0, "", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0, "", 1, "", 0, 0, "";
IPGroup 1 = 0, "Service_Provider", "Service_Provider", "",
"50.207.80.60", "", -1, 0, "DefaultSRD", "Public", "", 1, "Public", -1, -
1, -1, 0, 0, "", -1, "", 0, -1, -1, "", "Admin", "$1$aCkNBwIC", 0, "",
"", 0, "", "", 0, 0, "", 0, 0, -1, 0, 0, 1, "", -1, "", 0, 0, "", 1, "",
0, 0, "";

[ \IPGroup ]


[ ProxyIp ]

FORMAT Index = ProxySetId, ProxyIpIndex, IpAddress, TransportType,
Priority, Weight;
ProxyIp 0 = "0", 0, "10.64.110.212:5061", 2, 0, 0;
ProxyIp 1 = "1", 0, "50.207.80.60:5061", 2, 0, 0;

[ \ProxyIp ]


[ IP2IPRouting ]

FORMAT Index = RouteName, RoutingPolicyName, SrcIPGroupName,
SrcUsernamePrefix, SrcHost, DestUsernamePrefix, DestHost, RequestType,
MessageConditionName, ReRouteIPGroupName, Trigger, CallSetupRulesSetId,
DestType, DestIPGroupName, DestSIPInterfaceName, DestAddress, DestPort,
DestTransportType, AltRouteOptions, GroupPolicy, CostGroup, DestTags,
ModifiedDestUserName, SrcTags, IPGroupSetName, RoutingTagName,
InternalAction;
IP2IPRouting 0 = "Terminate Options", "Default_SBCRoutingPolicy", "Any",
"*", "*", "*", "*", 6, "", "Any", 0, -1, 1, "", "", "internal", 0, -1, 0,
0, "", "", "", "", "", "default", "";
IP2IPRouting 1 = "SM to SP", "Default_SBCRoutingPolicy",
"Session_Manager", "*", "*", "*", "*", 0, "", "Any", 0, -1, 0,
```

```
"Service_Provider", "", "", 0, -1, 0, 0, "", "", "", "", "", "default",
"";
IP2IPRouting 2 = "SP to SM", "Default_SBCRoutingPolicy",
"Service_Provider", "*", "*", "*", "*", 0, "", "Any", 0, -1, 0,
"Session_Manager", "", "", 0, -1, 0, 0, "", "", "", "", "", "default",
"";

[ \IP2IPRouting ]


[ GwRoutingPolicy ]

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

[ \GwRoutingPolicy ]


[ MaliciousSignatureDB ]

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

[ \MaliciousSignatureDB ]


[ AllowedAudioCoders ]

FORMAT Index = AllowedAudioCodersGroupName, AllowedAudioCodersIndex,
CoderID, UserDefineCoder;
AllowedAudioCoders 0 = "G.711 Only", 0, 1, "";
AllowedAudioCoders 1 = "G.711 Only", 1, 2, "";

[ \AllowedAudioCoders ]
```

```
[ AudioCoders ]

FORMAT Index = AudioCodersGroupId, AudioCodersIndex, Name, pTime, rate,
PayloadType, Sce, CoderSpecific;
AudioCoders 0 = "AudioCodersGroups_0", 0, 2, 2, 90, -1, 0, "";
AudioCoders 1 = "AudioCodersGroups_0", 1, 1, 2, 90, -1, 0, "";
AudioCoders 2 = "AudioCodersGroups_0", 2, 3, 2, 19, -1, 0, "";

[ \AudioCoders ]
```

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

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

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

Document #: LTRT-12265