



Avaya Solution & Interoperability Test Lab

Application Notes for AudioCodes MediaPack 1288 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes contain interoperability instructions for configuring AudioCodes MediaPack 1288 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Compliance testing was conducted to verify interoperability.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab in Thornton, CO.

Table of Contents

Table of Contents	2
1. Introduction.....	4
2. General Test Approach and Test Results.....	4
2.1. Interoperability Compliance Testing	4
2.2. Test Results.....	5
2.3. Support.....	5
3. Reference Configuration.....	6
4. Equipment and Software Validated	7
5. Configure Avaya Aura® Communication Manager.....	8
5.1. Verify Avaya Aura® Communication Manager License.....	8
5.2. Administer IP Network Region	9
5.3. Administer IP Codec Set	10
5.4. Administer IP Node Names	11
5.5. Administer SIP Signaling Group.....	12
5.6. Administer SIP Trunk Group.....	13
5.7. Administer Route Pattern	14
5.8. Administer Private Numbering.....	15
5.9. Administer AAR Analysis.....	15
6. Configure Avaya Aura® Session Manager	16
6.1. Add SIP Domain.....	17
6.2. Add Location	18
6.3. Add SIP Entity	19
6.4. Add Entity Link	20
6.5. Add Routing Policy	21
6.6. Add Dial Patterns.....	22
6.7. Add User.....	23
7. Configure AudioCodes MediaPack 1288	27
7.1. Verify/Upgrade Firmware Version.....	28
7.2. Administer Syslog Settings.....	29
7.3. IP Interfaces	30
7.4. Administer TLS Contacts	30
7.5. Media Realms	32
7.6. SIP Interfaces.....	33
7.7. Proxy Sets	34
7.8. Audio Coders Group.....	35
7.9. IP Profile.....	36
7.10. IP Groups	37
7.11. Trunk Group Settings.....	38
7.12. Trunk Groups	38
7.13. Tel-to-IP Routing	39
7.14. IP-to-Tel Routing	40

7.15.	Media Security	41
7.16.	Authentication	42
7.17.	Time and Date	42
8.	Verification Steps.....	43
9.	Conclusion	45
10.	Additional References.....	45
A.	Appendix.....	46

1. Introduction

AudioCodes MediaPack (MP) 1288 Analog VoIP gateways implement voice technology that connect analog telephones (FXS) to IP based PBX systems. In the compliance test, AudioCodes MP-1288 analog gateway was used to verify interoperability within an Avaya Aura® IP Telephony Environment.

The AudioCodes MP-1288 is a best-of-breed high density analog media gateway offering a cost-effective solution for organizations transitioning to all-IP that need to integrate large numbers of analog devices (such as legacy phones, fax machines and modems) into their new infrastructure.

- Ideal for VoIP deployments with large install base of analog devices
- Scalable solution with four capacity options: 288, 216, 144 and 72 ports
- Cost-effective - single management interface, single IP Address
- Reduced footprint - 3U chassis
- Designed for carrier-grade environments with 1+1 power supply modules and Ethernet redundancy
- Eliminate the need to stack and cable multiple small analog gateways

2. General Test Approach and Test Results

Interoperability compliance testing focused on verifying various inbound and outbound call flows between AudioCodes MP-1288, Communication Manager and Session Manager.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

Analog lines on AudioCodes MP-1288 were configured to register as SIP users on Session Manager. SIP TLS and SRTP were utilized during this test effort. The following features and functionalities were covered during compliance testing:

- Incoming calls to AudioCodes MP-1288
- Outgoing calls from AudioCodes MP-1288
- Voice codecs G.711U, G.711A and G.729 using SRTP
- DTMF tone transmission with RFC2833
- Calls using various Avaya endpoints, including analog, H.323 and SIP.
- Basic features including Hold/Resume, DTMF transmission, Voicemail with Message Waiting Indicator (MWI).

2.2. Test Results

All test cases were successfully executed.

2.3. Support

Technical support for AudioCodes MP-1288 can be obtained through the following:

- Phone:
 - Americas: +1-732-652-1085 or 1-800-735-4588
 - Rest of the World: 800-44422444 or 972-3-9764343
- Web: <https://services.audiocodes.com>
- E-Mail: support@audiocodes.com

3. Reference Configuration

The reference configuration consists of Communication Manager, Session Manager, System Manager, Messaging, AudioCodes MP-1288, and a number of Avaya telephones. AudioCodes MP-1288 is used as an analog gateway that connects analog endpoints to Avaya IP telephony network. The Session Manager in the right block, managed through the System Manager in the same block, routes the calls between the different entities using SIP Trunks.

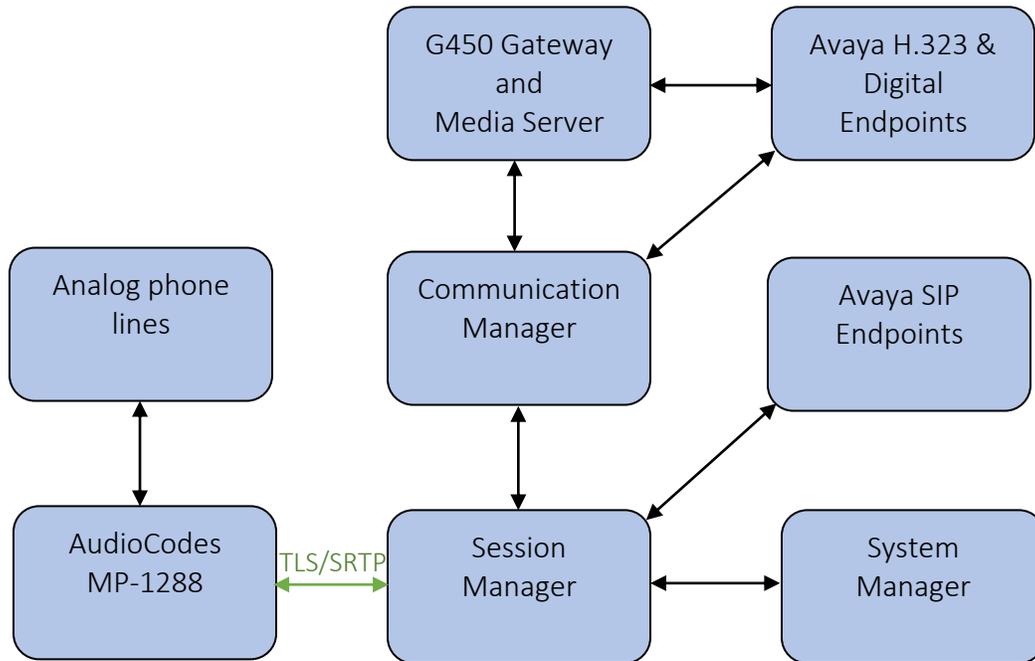


Figure 1: AudioCodes MP-1288 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Version
Avaya Aura® Communication Manager	8.1.1.0.0.890.25763
Avaya G450 Media Gateway	40.20.1
Avaya Aura® Session Manager	8.1.1.0.811021
Avaya Aura® System Manager	8.1.1.0.0310782
Avaya Aura® Media Server	8.0.2.61
Avaya 96x0 Series IP Telephones (H.323)	3.2.8
Avaya J100 Series Telephones (SIP)	4.0.4
Avaya 96x1 Series IP Telephones (H.323)	6.8.3
Avaya J100 Series Telephones (H.323)	
Avaya 96x1 Series IP Telephones (SIP)	7.1.7
Avaya one-X® Communicator (SIP)	6.2.10
Avaya Digital Telephone	-
AudioCodes MediaPack 1288	7.20A.256.511

5. Configure Avaya Aura® Communication Manager

This section provides steps for configuring Communication Manager. All configuration for Communication Manager is done through System Access Terminal (SAT).

5.1. Verify Avaya Aura® Communication Manager License

Use the **display system-parameters customer-options** command to verify options.

On **Page 2**, verify that there is sufficient capacity for SIP trunks by comparing **Maximum Administered SIP Trunks** field with corresponding **USED** column field.

```
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                  4
    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
```

On **Page 5**, verify **ISDN/PRI** and **Media Encryption Over IP** fields are set to **y**.

```
display system-parameters customer-options                               Page 5 of 12
                                OPTIONAL FEATURES

Emergency Access to Attendant? y                                     IP Stations? y
  Enable 'dadmin' Login? y
  Enhanced Conferencing? y                                         ISDN Feature Plus? y
    Enhanced EC500? y                                             ISDN/SIP Network Call Redirection? y
Enterprise Survivable Server? n                                     ISDN-BRI Trunks? y
  Enterprise Wide Licensing? n                                     ISDN-PRI? y
    ESS Administration? y                                         Local Survivable Processor? n
  Extended Cvg/Fwd Admin? y                                       Malicious Call Trace? y
  External Device Alarm Admin? y                                   Media Encryption Over IP? y
Five Port Networks Max Per MCC? n                                  Mode Code for Centralized Voice Mail? n
  Flexible Billing? n
Forced Entry of Account Codes? y                                   Multifrequency Signaling? y
  Global Call Classification? y                                   Multimedia Call Handling (Basic)? y
  Hospitality (Basic)? y                                           Multimedia Call Handling (Enhanced)? y
Hospitality (G3V3 Enhancements)? y                               Multimedia IP SIP Trunking? y
  IP Trunks? y

IP Attendant Consoles? y
```

5.2. Administer IP Network Region

Use the **change ip-network-region *n*** command to configure a network region, where *n* is an existing network region. Configure this network region as follows:

- Set **Location** to **1**
- Set **Codec Set** to **1**
- Set **Intra-region IP-IP Direct Audio** to **yes**
- Set **Inter-region IP-IP Direct Audio** to **yes**
- Enter an **Authoritative Domain**, e.g. **avaya.com**

```
change ip-network-region 1                                     Page 1 of 20
                                                           IP NETWORK REGION
Region: 1
Location: 1           Authoritative Domain: avaya.com
  Name: Main           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
DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46
  Audio PHB Value: 46
  Video PHB Value: 26
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
  Audio 802.1p Priority: 6
  Video 802.1p Priority: 5
H.323 IP ENDPOINTS           AUDIO RESOURCE RESERVATION PARAMETERS
  H.323 Link Bounce Recovery? y           RSVP Enabled? n
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
```

5.3. Administer IP Codec Set

Use the **change ip-codec-set *n*** command to configure IP codec set, where *n* is an existing codec set number. Configure this codec set as follows, on **Page 1**:

- Set **Audio Codec 1, 2** to **G.711MU, G.711A**, respectively.
- Set **Media Encryption 1** to **1-srtp-aescm128-hmac80**.

Note: G.711MU, G.711A and G.729AB were tested during compliance testing.

```
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.711A      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:
```

5.4. Administer IP Node Names

Use the **change node-names ip** command to add and entry for Session Manager. For compliance testing, **sm81** and **10.64.110.212** entries were added.

```
change node-names ip
```

Name	IP Address	IP NODE NAMES
aes81	10.64.110.215	
aes811	10.64.110.209	
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	

Page 1 of 2

5.5. Administer SIP Signaling Group

Use the **add signaling-group *n*** command to add a new signaling group, where *n* is an available signaling group number. Configure this signaling group as follows:

- Set **Group Type** to **sip**
- Set **Transport Method** to **TLS**
- Set **Near-end Node Name** to **procr**
- Set **Far-end Node Name** to the configured Session Manager in **Section 5.4**, i.e. **sm81**
- Set **Far-end Network region** to the configured region in **Section 5.2**, i.e. **1**
- Set **Direct IP-IP Audio Connections** to **y**

```
add signaling-group 1                                     Page 1 of 3
                                                         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: sm81
  Near-end Listen Port: 5061                          Far-end Listen Port: 5061
                                                         Far-end Network Region: 1

Far-end Domain:

Incoming Dialog Loopbacks: eliminate                  Bypass If IP Threshold Exceeded? n
  DTMF over IP: rtp-payload                          RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3                   Direct IP-IP Audio Connections? y
  Enable Layer 3 Test? y                             IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n               Initial IP-IP Direct Media? n
                                                         Alternate Route Timer(sec): 6
```

Note: The Signaling Group, Trunk Group and Route Pattern for PSTN calls via PRI were pre-configured and are not shown in this document

5.6. Administer SIP Trunk Group

Use the **add trunk-group *n*** command to add a trunk group, where *n* is an available trunk group number. Configure this trunk group as follows, on **Page 1**:

- Set **Group Type** to **sip**
- Enter a **Group Name**, e.g. **SM Trunk**
- Enter a valid **TAC**, e.g. **101**
- Set **Service Type** to **tie**
- Enter **Signaling Group** value to the signaling group configured in **Section 5.5**, i.e. **1**
- Enter a desired number in **Number of Members** field

```
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
```

On **Page 3**:

- Set **Number Format** to **private**

```
trunk-group 1                                       Page 3 of 5
TRUNK FEATURES
  ACA Assignment? n                                 Measured: both
                                               Maintenance Tests? y

  Suppress # Outpulsing? n  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
  Send UCID? y

  Show ANSWERED BY on Display? y
```

5.7. Administer Route Pattern

Use the **change route-pattern *n*** command to configure a route pattern, where *n* is an available route pattern. Configure this route pattern as follows:

- Type a name in **Pattern Name** field
- For line 1, set **Grp No** to the trunk group configured in **Section 5.6**, i.e. **1**
- For line 1, set **FRL** to **0**

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

5.8. Administer Private Numbering

Use the **change private-numbering 1** command to define the calling party number to send to Session Manager and configure private numbering as follows:

- Add entries for trunk group configured in **Section 5.6**

Note: For compliance testing, 5-digit extensions beginning with 7 routed over trunk group 1 which resulted in a 5-digit calling party number.

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

Ext  Ext      Trk      Private      Total
Len  Code     Grp(s)   Prefix      Len
 7   1         1                5   Total Administered: 1
                                Maximum Entries: 540
```

5.9. Administer AAR Analysis

Use the **change aar analysis n** command to configure routing for extensions starting with *n*. For compliance testing, extensions starting with **701** were used for AudioCodes MP-1288.

- Set **Dialed String** to starting digits of extensions that will be used, e.g. **701**
- Set **Min** and **Max** to **5** for 5 digit extensions
- Set **Route Pattern** to pattern configured in **Section 5.7**, i.e. **1**
- Set **Call Type** to **lev0**

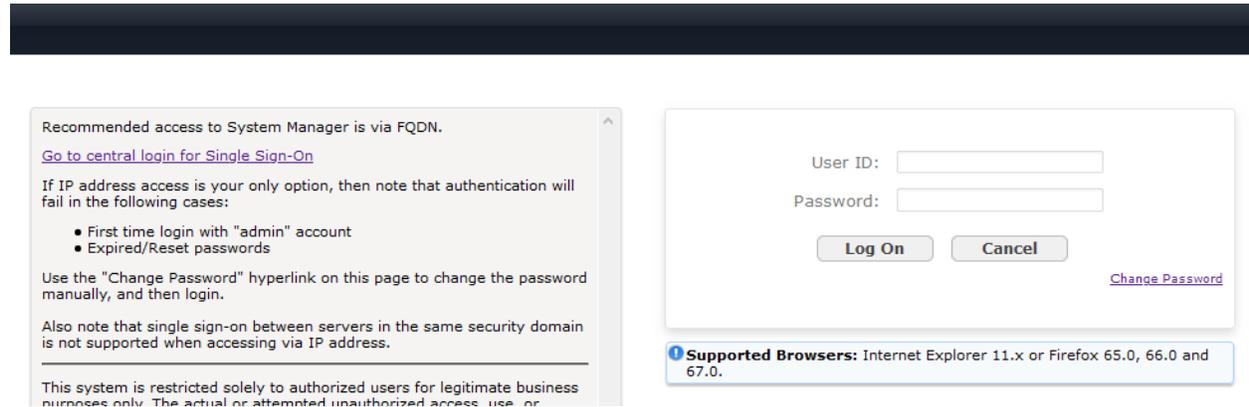
Note: An entry to dial plan will need to be added for extension range used in this step.

```
change aar analysis 701                                     Page 1 of 2
                                AAR DIGIT ANALYSIS TABLE
                                Location: all                Percent Full: 0

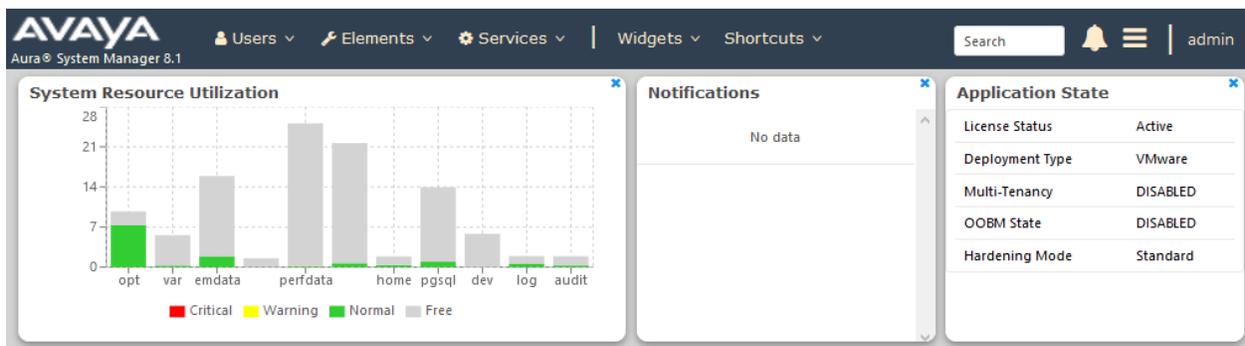
      Dialed      Total      Route      Call      Node      ANI
      String     Min  Max    Pattern  Type     Num     Reqd
    701           5   5     1         lev0     n
```

6. Configure Avaya Aura® Session Manager

Access the Session Manager Administration web interface by entering <https://<ip-address>/SMGR> URL in a web browser, where <ip-address> is the IP address of System Manager.



Log in using appropriate credentials

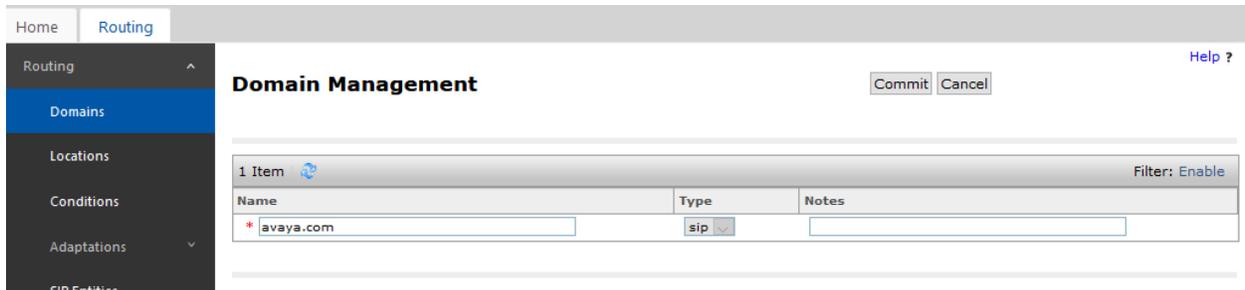


6.1. Add SIP Domain

Navigate to **Elements** → **Routing** → **Domains**, click on **New** button (not shown) and configure as follows:

- In **Name** field type in a domain (authoritative domain used in **Section 5.2**) i.e. **avaya.com**
- Set **Type** to **sip**

Click **Commit** to save changes.



The screenshot shows the 'Domain Management' interface. On the left is a navigation menu with 'Routing' selected, and 'Domains' highlighted. The main area is titled 'Domain Management' and contains a table with one item. The table has columns for 'Name', 'Type', and 'Notes'. The 'Name' column contains 'avaya.com', the 'Type' column contains 'sip', and the 'Notes' column is empty. There are 'Commit' and 'Cancel' buttons at the top right of the table area. A 'Filter: Enable' link is also visible.

Name	Type	Notes
* avaya.com	sip	

6.2. Add Location

Navigate to **Elements** → **Routing** → **Location**, click on **New** button (not shown) and configure as follows:

Under **General**:

- Type in a descriptive **Name**

At the bottom of the page, under **Location Pattern** click on **Add** (not shown):

- Type in **IP Address Pattern** for applicable subnets, e.g. **10.64.***

Click **Commit** to save changes.

The screenshot displays the 'Location Details' configuration page in the Avaya Element Manager. The page is divided into several sections:

- General:** Includes a text field for **Name** (value: DevConnect) and a **Notes** field.
- Dial Plan Transparency in Survivable Mode:** Features an **Enabled** checkbox (unchecked), a **Listed Directory Number** field, and an **Associated CM SIP Entity** field.
- Alarm Thresholds:** Includes **Multimedia Alarm Threshold** (80%), *** Latency before Overall Alarm Trigger** (5 Minutes), and *** Latency before Multimedia Alarm Trigger** (5 Minutes).
- Location Pattern:** A table with columns for selection, IP Address Pattern, and Notes. It contains one entry: * 10.64.*

Navigation and control elements include a breadcrumb trail (Home > Routing > Locations), a left-hand menu, and **Commit** and **Cancel** buttons at the top right and bottom right of the configuration area.

6.3. Add SIP Entity

Add Communication Manager as a SIP Entity. Navigate to **Elements** → **Routing** → **SIP Entities**, click on **New** (no shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Type in the IP address of FQDN of Communication Manager in **FQDN or IP Address** field.
- Set **Type** to **CM**
- Set **Location** to the location configured in **Section 6.2**

Click **Commit** to save changes

Note: It is assumed that SIP Entity for Session Manager has been already configured.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, user information (Users), and menu items for Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon (adm) are also present. The main content area is titled "SIP Entity Details" and is currently on the "General" tab. The configuration fields are as follows:

- Name:** cm81
- FQDN or IP Address:** 10.64.110.213
- Type:** CM
- Notes:** (empty field)
- Adaptation:** (empty dropdown)
- Location:** DevConnect
- Time Zone:** America/Denver

Buttons for "Commit" and "Cancel" are visible at the top right of the configuration area. A "Help ?" link is also present in the top right corner.

6.4. Add Entity Link

Navigate to **Elements** → **Routing** → **Entity Links**, click on **New** (not shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Set **SIP Entity 1** to the name of Session Manager SIP Entity
- Set **SIP Entity 2** to Communication Manager SIP Entity configured in **Section 6.3**

Click **Commit** to save changes.

The screenshot shows a web interface for configuring Entity Links. The breadcrumb navigation is Home > Routing > Entity Links. A left sidebar menu is open, showing options like Domains, Locations, Conditions, Adaptations, SIP Entities, and Entity Links (which is selected). The main content area is titled 'Entity Links' and contains a table with one row of configuration data. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, and Port. The values in the row are: Name: sm81_cm81_5061_TLS, SIP Entity 1: sm81, Protocol: TLS, Port: 5061, SIP Entity 2: cm81, and Port: 5061. There are 'Commit' and 'Cancel' buttons at the top right of the configuration area. A 'Filter: Enable' option is also visible.

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
<input type="checkbox"/>	* sm81_cm81_5061_TLS	* sm81	TLS	* 5061	* cm81	* 5061

6.5. Add Routing Policy

Navigate to **Elements** → **Routing** → **Routing Policies**, click on **New** (not shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Under **SIP Entity as Destination**, click on **Select**
 - Select Communication Manager SIP entity added in **Section 6.3**

Click **Commit** to save changes.

The screenshot shows the 'Routing Policy Details' configuration page. The left sidebar contains a navigation menu with 'Routing' selected. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' section, there are fields for 'Name' (cm81), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. Under the 'SIP Entity as Destination' section, there is a 'Select' button and a table with columns for Name, FQDN or IP Address, Type, and Notes. The table contains one entry: cm81, 10.64.110.213, CM.

Name	FQDN or IP Address	Type	Notes
cm81	10.64.110.213	CM	

6.6. Add Dial Patterns

Navigate to **Elements** → **Routing** → **Dial Patterns**, click on **New** (not shown) and configure as follows:

Under **General**:

- Set **Pattern** to prefix of dialed number
- Set **Min** to minimum length of dialed number
- Set **Max** to maximum length of dialed number

Under **Originating Locations and Routing Policies**:

Click **Add** and select originating location and Communication Manager routing policy. Click **Commit** to save changes (not shown).

Note: For Compliance testing, dialed number of 7xxxx were used.

The screenshot displays the 'Dial Pattern Details' configuration interface. The left sidebar contains navigation options: Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns (selected), and Origination Di... The main content area is titled 'Dial Pattern Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields: Pattern (7), Min (5), Max (5), Emergency Call (checkbox), SIP Domain (dropdown menu set to -ALL-), and Notes (text area). The 'Originating Locations and Routing Policies' section features an 'Add' button, a 'Remove' button, and a table with one item. The table has columns for Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes. The row shows Originating Location Name as '-ALL-', Routing Policy Name as 'cm81', Rank as 0, and Routing Policy Destination as 'cm81'. A 'Filter: Enable' link is present in the top right of the table area.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-		cm81	0	<input type="checkbox"/>	cm81	

6.7. Add User

For each analog line on AudioCodes MP-1288, a user needs to be added on Session Manager. Information in this section will be used by AudioCodes MP-1288 for registering to Session Manager.

Navigate to **Users → User Management → Manage User**, click on **New** (not shown) and configure as follows:

Under **Identity** tab:

- Type in **Last Name** and **First Name**
- In **Login Name** field type in <extension>@<domain>. <Extension> is an extension which will be configured on AudioCodes MP-1288 to receive and make calls. <domain> is as configured in **Section 6.1**

Home / Users / Manage Users Help ?

User Profile | Add

Identity | Communication Profile | Membership | Contacts

Basic Info

Address

LocalizedName

User Provisioning Rule:

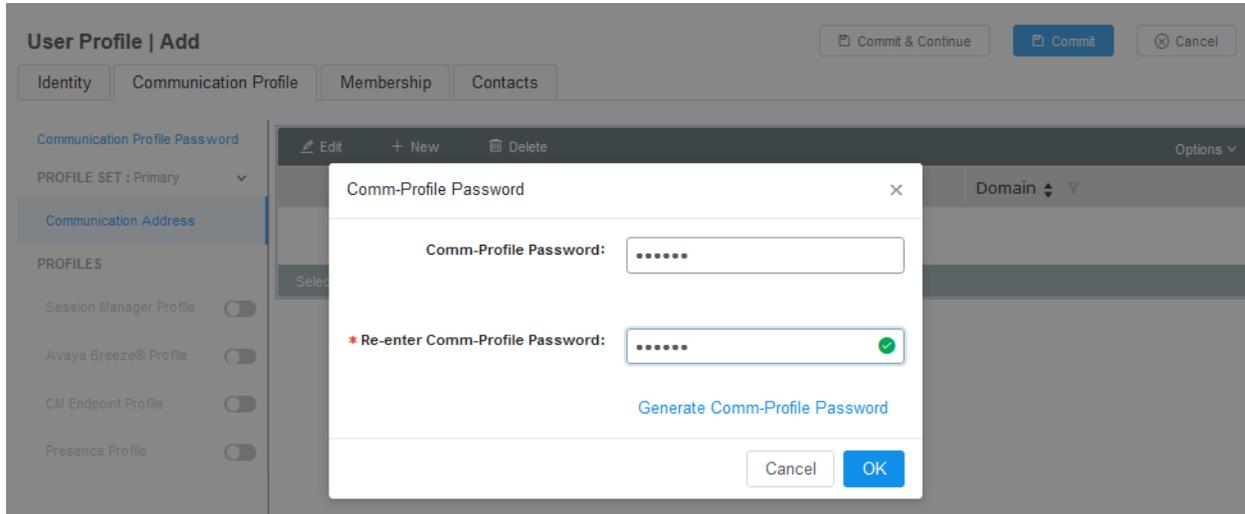
* Last Name: Last Name (in Latin alphabet characters):

* First Name: First Name (in Latin alphabet characters):

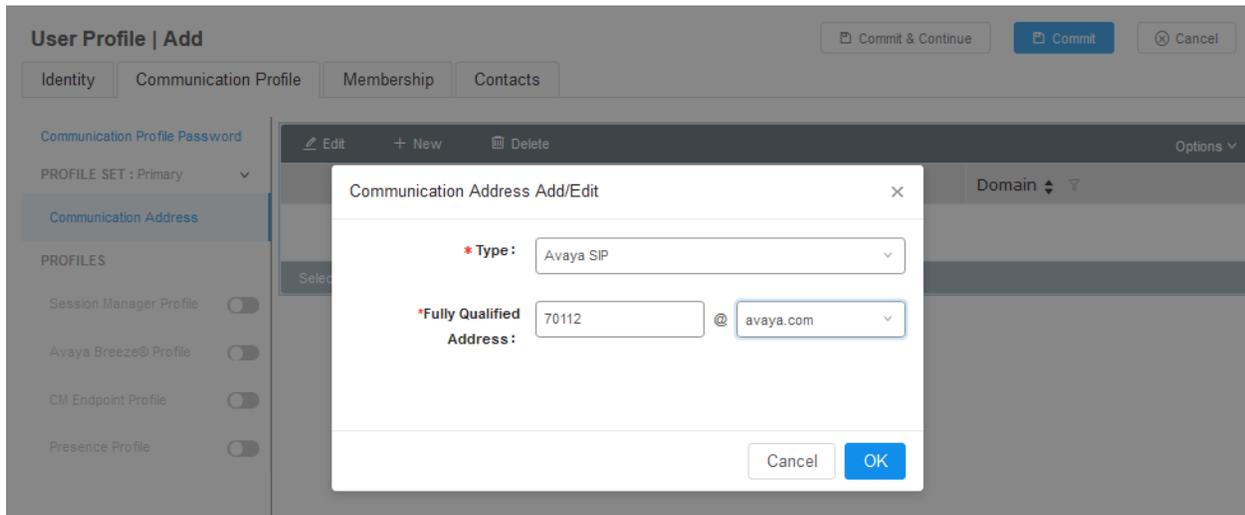
* Login Name: Middle Name:

Under **Communication Profile** tab:

- Under **Communication Profile**, select **Communication Profile Password** and fill in **Password** details. This password will be used by AudioCodes MP-1288 to log in.



- Under **Communication Address** sub-section, click on **New**
 - Set **Type** to **Avaya SIP**
 - Type in <extension> in the text field, select domain configured in **Section 6.1** for **Fully Qualified Address**. <Extension> is the same extension configured for login name under Identity tab. Click on **Add**. Please note that AudioCodes MP-1288 will use this information as login name to register to Session Manager



- Toggle the **Session Manager Profile** button to turn it on:
 - Set **Primary Session Manager** to Session Manager. i.e. sm81
 - Set **Origination Application Sequence** and **Termination Application Sequence** to Communication Manager entity. Please note that configuration for Application Sequence is not shown in this document. Please refer to document [2] in reference section of this document for further details.
 - Set **Home Location** (not shown)

Identity
Communication Profile
Membership
Contacts

Communication Profile Password

PROFILE SET : Primary ▼

Communication Address

PROFILES

Session Manager Profile 🔴

Avaya Breeze® Profile 🔴

CM Endpoint Profile 🔴

Presence Profile 🔴

SIP Registration

*** Primary Session Manager:** 🔍 ⓘ

Secondary Session Manager: 🔍 ⓘ

Survivability Server: 🔍 ⓘ

Max. Simultaneous Devices: ▼

Block New Registration When Maximum Registrations Active?

Application Sequences

Origination Sequence: ▼

Termination Sequence: ▼

- Toggle **CM Endpoint Profile** button to turn it on:
 - Set **System** to Communication Manager entity
 - Set **Profile Type** to **Endpoint**
 - Type in extension number used in this section for **Extension** field
 - Set **Template** to **9641SIP_DEFAULT_CM_8_1**

User Profile | Add Commit & Continue **Commit** Cancel

Identity **Communication Profile** Membership Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

CM Endpoint Profile

* System: cm81

* Profile Type: Endpoint

Use Existing Endpoints:

* Extension: 70111

* Template: 9641SIP_DEFAULT_CM_8_1

* Set Type: 9641SIP

Security Code: Enter Security Code

Port: jp

Voice Mail Number:

Preferred Handle: Select

Click **Commit** to save changes.

Two SIP Users for AudioCodes MP-1288 were configured during the Compliance test.

Home Routing **User Management** Help

User Management Manage Users

Search

View	Edit	New	Duplicate	Delete	More Actions	Options
First Name	Surname	Display Name	Login Name	SIP Handle		
<input type="checkbox"/>	User 1	AudioCodes	AudioCodes, User 1	70111@avaya.com	70111	
<input type="checkbox"/>	User 2	AudioCodes	AudioCodes, User 2	70112@avaya.com	70112	
<input type="checkbox"/>	admin	admin	Default Administrator	admin		
<input type="checkbox"/>	SIP	Station 1	Station 1, SIP	70101@avaya.com	70101	
<input type="checkbox"/>	SIP	Station 2	Station 2, SIP	70102@avaya.com	+70102	
<input type="checkbox"/>	SIP	Station 3	Station 3, SIP	70103@avaya.com	70103	
<input type="checkbox"/>	SIP	Station 4	Station 4, SIP	70104@avaya.com	70104	
<input type="checkbox"/>	H323 1	Station	Station, H323 1	70001@avaya.com	70001	

7. Configure AudioCodes MediaPack 1288

Administration for AudioCodes MP-1288 series is done via an administrative console. Type in <http://<ip-address>> URL in a web browser, where <ip-address> is the IP Address of AudioCodes MP-1288. It is assumed that AudioCodes MP-1288 has been assigned an IP Address and initial configuration has already been performed.

Log on to administrative console using appropriate credentials.



Web Login

Username

Password

Remember Username

7.1. Verify/Upgrade Firmware Version

Once logged in, select **MONITOR** and verify that the firmware version is **7.20A.256.511** or higher. If firmware needs to be upgraded, navigate to **SETUP → ADMINISTRATION → MAINTENANCE → Software Upgrade** and select **Start Software Upgrade** (not shown).

The screenshot shows the Audiocodes web interface for monitoring an MP-1288 FXS device. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The 'MONITOR' tab is active. The page displays the following information:

- Device Address: 10.64.10.28
- Firmware Version: 7.20A.256.511 (highlighted in a red box)
- Device Type: MP-1288 FXS
- S/N: 12369647

The 'Alarms' section contains a table with the following data:

Alarm ID	Component	Status	Value	Port	Category
S1	CPU	OK	72 FXS ports	S1	Sys
S2	GE-1	OK		S2	Tel
S3	GE-2	OK		S3	Power
S4	PS	OK	1	S4	Fan

7.2. Administer Syslog Settings

Syslog can be enabled for troubleshooting purposes. Navigate to **System** → **Syslog Settings**

- Set **Enable Syslog** to **Enable**
- For **Syslog Server IP** Address, type in the IP address of a workstation that is running a syslog application, e.g. **ACSyslog**
- Set **Log Severity Level** to **Debug**
- Set **VoIP Debug Level** to **Detailed**

Click **Apply** to save changes (not shown).

The screenshot shows the Audiocodes MP-1288 FXS Troubleshoot interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The 'TROUBLESHOOT' section is active, showing 'MP-1288 FXS' and 'TROUBLESHOOT' tabs. A search bar contains 'Entry, parameter, va'. Below the navigation, there are navigation icons and a dropdown menu set to 'All'. The main content area is titled 'Logging Settings' and is divided into two columns: 'SYSLOG' and 'ACTIVITY TYPES TO REPORT'. The 'SYSLOG' column contains several settings, with four highlighted by red boxes: 'Enable Syslog' (set to 'Enable'), 'Syslog Server IP' (set to '10.64.10.47'), 'Log Severity Level' (set to 'Debug'), and 'VoIP Debug Level' (set to 'Detailed'). The 'ACTIVITY TYPES TO REPORT' column lists various activity types with checkboxes, all of which are checked.

SYSLOG	
Enable Syslog	Enable
Syslog Server IP	10.64.10.47
Syslog Server Port	514
Log Severity Level	Debug
Syslog CPU Protection	Enabled
Syslog Optimization	Disabled
VoIP Debug Level	Detailed
Debug Level High Threshold	90

ACTIVITY TYPES TO REPORT	
Select All	<input checked="" type="checkbox"/>
Parameters Value Change	<input checked="" type="checkbox"/>
Auxiliary Files Loading	<input checked="" type="checkbox"/>
Device Reset	<input checked="" type="checkbox"/>
Flash Memory Burning	<input checked="" type="checkbox"/>
Device Software Upgrade	<input checked="" type="checkbox"/>
Non-Authorized Access	<input checked="" type="checkbox"/>
Sensitive Parameters Value Change	<input checked="" type="checkbox"/>
Login and Logout	<input checked="" type="checkbox"/>
CLI Activity	<input checked="" type="checkbox"/>
Action Executed	<input checked="" type="checkbox"/>

7.3. IP Interfaces

From the configuration menu at the top, navigate to **IP NETWORK → CORE ENTITIES → IP Interfaces**. During the compliance test, the IP Interface was configured as follows:

#0[mp1288.avaya.com]

[Edit](#)

GENERAL		IP ADDRESS	
Name	• mp1288.avaya.com	Interface Mode	IPv4 Manual
Application Type	OAMP + Media + Control	IP Address	• 10.64.10.28
Ethernet Device	• vlan 1 View	Prefix Length	• 24
DNS		Default Gateway	• 10.64.10.1
Primary DNS	• 10.64.110.100		
Secondary DNS	• 75.75.75.75		

7.4. Administer TLS Contexts

In order for TLS/SRTP to work correctly with Session Manager, a TLS context needs to be configured. Navigate to **SETUP → IP NETWORK → SECURITY → TLS Contexts** and select + **New** to add a new TLS Context. The following was created during the compliance test to be used by System Manager to sign the AudioCodes MP-1288 certificate.

#1[audiocodes1288]

[Edit](#)

GENERAL		OCSP	
Name	• audiocodes1288	OCSP Server	Disable
TLS Version	TLSv1.0 TLSv1.1 and TLSv1.2	Primary OCSP Se...	0.0.0.0
DTLS Version	Any	Secondary OCSP...	0.0.0.0
Cipher Server	DEFAULT	OCSP Port	2560
Cipher Client	DEFAULT	OCSP Default Re...	Reject
Strict Certificate ...	Disable		
DH key Size	• 2048		
TLS Renegotiation	Enable		

[Certificate Information >>](#)

[Change Certificate >>](#)

[Trusted Root Certificates >>](#)

Select **Change Certificate** and fill in the needed information and **Create CSR**.

CERTIFICATE SIGNING REQUEST

Common Name [CN]	<input type="text" value="audiocodes1288"/>
Organizational Unit [OU] <i>(optional)</i>	<input type="text" value="DevConnect"/>
Company name [O] <i>(optional)</i>	<input type="text" value="Avaya"/>
Locality or city name [L] <i>(optional)</i>	<input type="text" value="Thronton"/>
State [ST] <i>(optional)</i>	<input type="text" value="CO"/>
Country code [C] <i>(optional)</i>	<input type="text" value="US"/>
1st Subject Alternative Name [SAN]	<input type="text" value="EMAIL"/> ▼
2nd Subject Alternative Name [SAN]	<input type="text" value="EMAIL"/> ▼
3rd Subject Alternative Name [SAN]	<input type="text" value="EMAIL"/> ▼
4th Subject Alternative Name [SAN]	<input type="text" value="EMAIL"/> ▼
5th Subject Alternative Name [SAN]	<input type="text" value="EMAIL"/> ▼
Signature Algorithm	<input type="text" value="SHA-256"/> ▼

The generated CSR will be signed by System Manager and a **Device Certificate** will be generated (not shown). At the bottom of the page, **Browse** to the certificate generated by System Manager and type in the password used during the certificate generation in **Private key pass-phrase**. Select **Load File** to add the certificate to the device. Note that when the **Device Certificate** is loaded, the root certificate of System Manager is also added as a trusted certificate.

UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

Private key pass-phrase *(optional)*

Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

No file selected.

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

Send **Device Certificate** file from your computer to the device.
The file must be in textual PEM format.

audiocodes1288avayacom.pem

7.5. Media Realms

From the configuration menu at the top, navigate to **SIGNALING & MEDIA → CORE ENTITIES → Media Realms**. During the compliance tests, the default Media Realms were used as shown below.

Media Realms (1)

[+ New](#) [Edit](#)  Page 1 of 1 Show 10 records per page

INDEX	NAME	IPV4 INTERFACE NAME	UDP PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	UDP PORT RANGE END	DEFAULT MEDIA REALM
0	DefaultRealm	mp1288.avaya.com	6000	5953	65529	Yes

7.6. SIP Interfaces

Select **SIP Interfaces** on the left and add a SIP Interface for the Session Manager. Configure the SIP Interface for Session Manager as shown below:

- **Name:** Provide a descriptive name.
- **Network Interface:** Select the private interface from **Section 7.3**.
- **TLS Context:** Select the TLS Context configured in **Section 7.4**.

Retain default values for the rest of the fields.

#0[SIPInterface_0] DefaultSRD

[Edit](#)

GENERAL	
Name	• SIPInterface_0
Topology Location	Down
Network Interface	• mp1288.avaya.com View
Application Type	GW
UDP Port	• 0
TCP Port	• 0
TLS Port	5061
Additional UDP P...	
Additional UDP P...	Always Open
Encapsulating Pr...	No encapsulation
Enable TCP Keep...	Disable
Used By Routing ...	Not Used
Pre-Parsing Mani...	-- View
CAC Profile	-- View

MEDIA	
Media Realm	-- View
Direct Media	Disable

SECURITY	
TLS Context Na...	• audiocodes1288 View
TLS Mutual Auth...	
Message Policy	-- View
User Security M...	Not Configured
Enable Un-Authe...	Not configured
Max. Number of ...	-1

7.7. Proxy Sets

Select **Proxy Sets** on the left. Add a Proxy Sets for Session Manager and configure as shown below:

- **Name:** Provide a descriptive name.
- **Gateway IPv4 SIP Interface:** Select the SIP Interface from **Section 7.6**.
- **TLS Context Name:** Select the TLS Context configured in **Section 7.4**.

#0[ProxySet_0] DefaultSRD Edit

GENERAL	
Name	• ProxySet_0
Gateway IPv4 SIP...	• SIPInterface_0 View
TLS Context Name	• audiocodes1288 View

REDUNDANCY	
Redundancy Mo...	
Proxy Hot Swap	Disable
Proxy Load Bala...	Disable
Min. Active Serv...	1

KEEP ALIVE	
Proxy Keep-Alive	Disable
Proxy Keep-Alive ...	60
Keep-Alive Failure...	
Success Detectio...	1
Success Detectio...	10
Failure Detection ...	-1

ADVANCED	
Classification Inp...	IP Address only
DNS Resolve Me...	

PROXY ADDRESS	TYPE
10.64.110.212	TLS

[Proxy Address 1 items >>](#)

Continuing from above, select **Proxy Address items**. Select + **New** to a new Proxy Address. For **Proxy Address** field, type the Session Manager SIP security module IP Address and select **Transport Type** of **TLS** from the drop-down menu. The following was configured during the compliance test.

#0 Edit

GENERAL	
Proxy Address	• 10.64.110.212
Transport Type	• TLS
Proxy Priority	0
Proxy Random W...	0

7.8. Audio Coders Group

Select **CODERS & PROFILE** → **Coders Groups** on the left and configure the Coders as shown below:

TOPOLOGY VIEW

- CORE ENTITIES
- CODERS & PROFILES**
 - IP Profiles (1)
 - Tel Profiles (0)
 - Coder Settings
 - Coder Groups**
- GATEWAY
- SIP DEFINITIONS
- MESSAGE MANIPULATION
- MEDIA
- INTRUSION DETECTION

Coder Groups

Coder Group Name:

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

7.9. IP Profile

Select **CODERS & PROFILE** → **IP Profiles** on the left. Add an IP Profile for Session Manager and configure as shown below:

- **Name:** Provide a descriptive name (not shown).
- **Coders Group:** Select the Audio Coder Group from **Section 7.8**.

#1[Session_Manager]

Edit

GENERAL	
Name	• Session_Manager
Created by Routi...	No

MEDIA SECURITY	
Gateway Media S...	Mandatory
Symmetric MKI	Disable
MKI Size	0
Reset SRTP Upon...	Disable
Generate SRTP K...	Only If Required

SBC MEDIA	
SBC Multiple Cod...	Not Supported

QUALITY OF SERVICE	
--------------------	--

SBC SIGNALING	
MSRP Empty Me...	Default

MEDIA	
Broken Connect...	Disconnect
Media IP Version...	Only IPv4
RTP Redundancy...	Disable

GATEWAY	
Early Media	Enable
Early 183	Disable
Early Answer Ti...	0
Profile Preference	1
Coders Group	• AudioCodersGroups_0
Play RB Tone to IP	Disable

7.10. IP Groups

Select **CORE ENTITIES** → **IP Groups** on the left. During the compliance test, the default IP Group was used for Session Manager. It was configured as shown below:

- **Name:** Provide a descriptive name.
- **Proxy Set:** Select the Proxy set from **Section 7.7**.
- **IP Profile:** Select the IP Profile from **Section 7.9**.
- **Media Realm:** Select the Media Realm from **Section 7.5**.
- **Internal Media Realm:** Select the Media Realm from **Section 7.5**.
- **SIP Group Name:** Type in the SIP Domain of Session Manager.
- **Proxy Keep-Alive:** Select **Enable** from the drop-down menu.

#0[Default_IPG] DefaultSRD

[Edit](#)

GENERAL	
Name	• Default_IPG
Topology Location	Down
Proxy Set	• ProxySet_0 View
IP Profile	• Session_Manager View
Media Realm	• DefaultRealm View
Internal Media Re...	• DefaultRealm View
Contact User	
SIP Group Name	• avaya.com
Created By Routi...	No
Used By Routing ...	Not Used
Proxy Set Connec...	NA

QUALITY OF EXPERIENCE	
QoE Profile	-- View
Bandwidth Profile	-- View

MESSAGE MANIPULATION	
Inbound Messa...	-1
Outbound Mess...	-1
Message Manipu...	
Message Manipu...	
Proxy Keep-Alive...	• Enable

SBC REGISTRATION AND AUTHENTICATION	
-------------------------------------	--

7.11. Trunk Group Settings

Select **Gateway → Trunk & Groups → Trunk Group Settings** on the left. Add a new Trunk Group as shown below. This trunk group will be assigned the analog channels.

- **Name:** Provide a descriptive name
- **Trunk Group ID:** Enter an available trunk group ID
- **Channel Select Mode:** Set to **By Dest Phone Number**
- **Registration Mode:** Set to **Per Endpoint**
- **Serving IP Group:** Set to the IP Group from **Section 7.10**.

#0[TrunkGroup-1]

[Edit](#)

GENERAL		SIP CONFIGURATION	
Name	• TrunkGroup-1	Gateway Name	
Trunk Group ID	• 1	Contact User	
Channel Select ...	• By Dest Phone Number	Serving IP Group	• Default_IPG View
Registration Mode	• Per Endpoint	Dedicated Conn...	Reuse Connection
Used By Routing ...	Not Used	MWI Interrogati...	

STATUS	
Admin State	Unlocked
Status	

7.12. Trunk Groups

Select **Gateway → Trunk & Groups → Trunk Group** on the left. Assign the Trunk Group channels to the trunk group. Two channels were used during the compliance test and it was configured as shown below. Note that the SIP Users configured in **Section 6.7** were configured here.

Trunk Group Table

Add Phone Context As Prefix Disable

Trunk Group Index 1-12

Group Index	FXS Blade	Channels	Phone Number	Trunk Group ID	Tel Profile Name
1	FXS Blade 1	1	70111	1	None
2	FXS Blade 1	2	70112	1	None
3					None

7.13. Tel-to-IP Routing

Select **Gateway** → **Routing** → **Tel-to-IP Routing** on the left. Configure the routing from AudioCodes MP-1288 to Session Manager as shown below:

- **Name:** Provide a descriptive name
- **Source Trunk Group:** Trunk group from **Section 7.11**
- **SIP Interface:** SIP Interface from **Section 7.6.**
- **Destination IP Address:** Set to the SIP IP Address of Session Manager
- **Destination Port:** Set to the port configured in **Section 6.4**
- **Transport Type:** Set to **TLS**

#0[Tel to Ip]

[Edit](#)

GENERAL	
Name	• Tel to Ip
Connectivity Status	Not Available

MATCH	
Source Trunk Gr...	• 1
Source Phone Pat...	*
Source Tag	
Destination Pho...	*
Destination Tag	

ACTION	
Destination IP G...	-- View
SIP Interface	• SIPInterface_0 View
Destination IP A...	• 10.64.110.212
IP Profile	-- View
Destination Port	• 5061
Transport Type	• TLS

ADVANCED	
Call Setup Rules ...	-1
Forking Group	-1
Cost Group	-- View
Charge Code	-- View

7.14. IP-to-Tel Routing

Select **Gateway** → **Routing** → **IP-to-Tel Routing** on the left. Configure the routing from Session Manager to AudioCodes MP-1288 as shown below:

- **Name:** Provide a descriptive name
- **Source SIP Interface:** SIP Interface from **Section 7.6**
- **Trunk Group ID:** Trunk Group IP from **Section 7.11**

#0[IP to Tel]

Edit

GENERAL	
Name	• IP to Tel

MATCH	
Source SIP Interfa...	• SIPInterface_0 View
Source IP Address	*
Source Phone Pat...	*

ACTION	
Destination Type	Trunk Group
Trunk Group ID	• 1
Source IP Group	-- View
IP Profile	-- View
Trunk ID	-1
Call Setup Rules ...	-1

7.15. Media Security

Select **MEDIA** → **Media Security** on the left; set **Media Security** to **Enable** and **Media Security Behavior** to **Mandatory**.

Media Security			
GENERAL	AUTHENTICATION & ENCRYPTION		
Media Security	• Enable <input type="text"/>	Authentication on Transmitted RTP Packets	Active <input type="text"/>
Media Security Behavior	• Mandatory <input type="text"/>	Encryption on Transmitted RTP Packets	Active <input type="text"/>
Offered SRTP Cipher Suites	All <input type="text"/>	Encryption on Transmitted RTCP Packets	• Inactive <input type="text"/>
ARIA Protocol Support	Disable <input type="text"/>	SRTP Tunneling Authentication for RTP	Disable <input type="text"/>
		SRTP Tunneling Authentication for RTCP	Disable <input type="text"/>

7.16. Authentication

SIP Users added in Session Manager need to be added on AudioCodes MP-1288. Each SIP User will be assigned to a channel. Navigate to **Gateway → Analog Gateway → Authentication**. The two SIP Users and Passwords from **Section 6.7** are configure as shown below.

INDEX	MODULE	PORT	PORT TYPE	USER NAME	PASSWORD
0	1	1	FXS	70111	*
1	1	2	FXS	70112	*
2	1	3	FXS		
3	1	4	FXS		
4	1	5	FXS		
5	1	6	FXS		
6	1	7	FXS		
7	1	8	FXS		
8	1	9	FXS		
9	1	10	FXS		

7.17. Time and Date

Navigate to **SETUP → ADMINISTRATION → TIME & DATE**.

- **Enable NTP:** Select **Enable** from the drop-down menu.
- **Primary NTP Server Address:** Type in a designated NTP Server.

LOCAL TIME							TIME ZONE					
Local Time	Year	Month	Day	Hours	Minutes	Seconds	UTC Time	30 Mar, 2020 22:30:04				
	2020	3	30	22	30	4	UTC Offset	Hours: 0	Minutes: 0			
NTP SERVER							Daylight Saving Time	Disable				
Enable NTP	Enable						DST Mode	Day of year				
Primary NTP Server Address (IP or FQDN)	0.rhel.pool.ntp.org						Start Time	Jan	01	0	: 0	
Secondary NTP Server Address (IP or FQDN)							End Time	Jan	01	0	: 0	
NTP Update Interval	Hours: 24	Minutes: 0					Offset [min]	60				
NTP Authentication Key Identifier	0						Day of Month Start	Jan	Sunday	First	0	: 0
NTP Authentication Secret Key							Day of Month End	Jan	Sunday	First	0	: 0

8. Verification Steps

- Verify SIP trunks to Session Manager are in service via SAT, using **status trunk n**, where n is the number of the trunk configured in **Section 6**. Service State column should show **in-service/idle**.

```
status trunk 1

                                TRUNK GROUP STATUS

Member   Port      Service State   Mtce Connected Ports
                                Busy

0001/001 T00001   in-service/idle no
0001/002 T00002   in-service/idle no
0001/003 T00003   in-service/idle no
0001/004 T00004   in-service/idle no
0001/005 T00005   in-service/idle no
0001/006 T00006   in-service/idle no
0001/007 T00007   in-service/idle no
0001/008 T00008   in-service/idle no
0001/009 T00009   in-service/idle no
0001/010 T00010   in-service/idle no
```

- Verify SIP Users (from **Section 6.7**) registration from AudioCodes MP-1288 to Session Manager via System Manager console, <http://<ip-address>/SMGR>
- Navigate to **Home** → **Session Manager** → **System Status** → **User Registration**

User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

AST Device Notifications: Reboot Reload Failback As of 4:32 PM												Registered		
View	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered			
											Prim	Sec	Surv	
<input type="checkbox"/>	Show	70112@avaya.com	User 2	AudioCodes	DevConnect	10.64.10.28	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	Show	70111@avaya.com	User 1	AudioCodes	DevConnect	10.64.10.28	<input type="checkbox"/>	<input type="checkbox"/>	1/10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	Show	70103@avaya.com	SIP	Station 3	DevConnect	10.64.10.47	<input type="checkbox"/>	<input type="checkbox"/>	2/10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	Show	70103@avaya.com	SIP	Station 3	DevConnect	10.64.10.205	<input type="checkbox"/>	<input type="checkbox"/>	2/10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	Show	70101@avaya.com	SIP	Station 1	DevConnect	10.64.10.201	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	Show	---	SIP	Station 2	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	Show	---	SIP	Station 4	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Select : All, None

9. Conclusion

These Application Notes describe the configuration steps required for AudioCodes MP-1288 to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. All feature and serviceability test cases completed and pass with observations/exceptions noted in **Section 2.2**

10. Additional References

Avaya references are available at <http://support.avaya.com>

- [1] “Administering Avaya Aura® Session Manager”, Release 8.1.1, October 2019
- [2] “Administering Avaya Aura® Communication Manager”, Release 8.1.x, Issue 5, November 2019

AudioCodes MP-1288 references can directly be obtained from AudioCodes.

A. Appendix

AudioCodes MP-1288 .ini file generated during the compliance testing is as follows: Please use it only for reference purposes.

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

;Time & Date: 30/03/2020 22:37:39
;Device Up Time: 2d:22h:36m:53s
;Board: MP-1288 FXS
;Board Type: 86
;Serial Number: 12369647
;Product Key: DT3507405
;Software Version: 7.20A.256.511
;DSP Software Version: 5033AE3_R => 723.04
;Board IP Address: 10.64.10.28
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 10.64.10.1
;CPU: Cavium Networks Octeon V0.1 @ 700Mhz, total 2 cores, 2 cpus, 1 sockets
;Cores mapping:
;core #0, on cpu #0, on socket #0
;core #1, on cpu #1, on socket #0
;Memory: 1024 MB
;Flash size: 128 MB
;Num of DSP Cores: 6
;Num of physical LAN ports: 2
;;;Key features::;Board Type: MP-1288 FXS ;Coders: G723 G729 G727 G722 ;DSP
Voice features: IpmDetector ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;System features: ProducrKey=DT3507405 ;PSTN
Protocols: CAS ;Channel Type: RTP DspCh=312 ;IP Media: VXML ;Control
Protocols: SIP MSFT EMS ;Default features::;Coders: G711 G726;

;----- HW components -----
;
; Slot # : Module type : # of ports
;-----
;      1 : FXS           : 72
;      2 : Empty
;      3 : Empty
;      4 : Empty
;-----

;USB Port 1: Empty
;Power Supply 1: Exists
;Power Supply 2: Not Exists
;Fan Tray: Exists
;-----

[SYSTEM Params]

SyslogServerIP = 10.64.10.47
```

```
EnableSyslog = 1
ENABLEPARAMETERSMONITORING = 1
ActivityListToLog = 'pvc', 'afl', 'dr', 'fb', 'swu', 'naa', 'spc', 'll',
'cli', 'ae'
TLSPkeySize = 2048
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
NTPServerIP = '0.rhel.pool.ntp.org'
SyslogLogLevel = 7
PM_VEDSPUtil = '1,280,312,15'
```

[BSP Params]

```
PCMLawSelect = 3
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95
```

[Analog Params]

```
PolarityReversalType = 1
MinFlashHookTime = 100
```

[ControlProtocols Params]

```
AdminStateLockControl = 0
```

[Voice Engine Params]

```
FaxTransportMode = 0
V22ModemTransportType = 0
V23ModemTransportType = 0
V32ModemTransportType = 0
V34ModemTransportType = 0
RFC2833TxPayloadType = 101
V34FAXTRANSPORTTYPE = 0
RTCPEncryptionDisableTx = 1
ENABLEMEDIASECURITY = 1
PLThresholdLevelsPerMille_0 = 5
PLThresholdLevelsPerMille_1 = 10
PLThresholdLevelsPerMille_2 = 20
PLThresholdLevelsPerMille_3 = 50
CallProgressTonesFilename = 'usa_tones_13.dat'
```

[WEB Params]

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

[SIP Params]

```
ISREGISTERNEEDED = 1
SIPDESTINATIONPORT = 5061
GWDEBUGLEVEL = 5
ENABLEEARLYMEDIA = 1
SIPGATEWAYNAME = 'avaya.com'
ENABLEMWISUBSCRIPTION = 1
```

```
MWISERVERIP = '10.64.110.212'  
MWIANALOGLAMP = 1  
MWIDISPLAY = 1  
ENABLEMWI = 1  
ENABLESIPS = 1  
MEDIASECURITYBEHAVIOUR = 1  
MWISERVERTRANSPORTTYPE = 2  
MSLDAPPRIMARYKEY = 'telephoneNumber'  
ENERGYDETECTORCMD = 587202560  
ANSWERDETECTORCMD = 10486144
```

```
[SNMP Params]
```

```
[ 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_1";
```

```
[ \PhysicalPortsTable ]
```

```
[ EtherGroupTable ]
```

```
FORMAT Index = Group, Mode, Member1, Member2;  
EtherGroupTable 0 = "GROUP_1", 2, "GE_1", "GE_2";  
EtherGroupTable 1 = "GROUP_2", 0, "", "";
```

```
[ \EtherGroupTable ]
```

```
[ DeviceTable ]
```

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

```
[ \DeviceTable ]
```

```
[ InterfaceTable ]
```

```
FORMAT Index = ApplicationTypes, InterfaceMode, IPAddress, PrefixLength,  
Gateway, InterfaceName, PrimaryDNSServerIPAddress,  
SecondaryDNSServerIPAddress, UnderlyingDevice;  
InterfaceTable 0 = 6, 10, 10.64.10.28, 24, 10.64.10.1, "mp1288.avaya.com",  
10.64.110.100, 75.75.75.75, "vlan 1";
```

```
[ \InterfaceTable ]
```

```
[ WebUsers ]
```

```
FORMAT Index = Username, Password, Status, PwAgeInterval, SessionLimit,  
CliSessionLimit, SessionTimeout, BlockTime, UserLevel, PwNonce, SSHPublicKey;
```

```
WebUsers 0 = "Admin",
"$1$VTEzY2o4aWNqad86UlkAVQUDB14LDQ4JD1ReXUJBRhYRFxRGHh8YSk0YSE7iuOextrO/vuvtv
O/qu77rpajw8K0=", 1, 0, 5, -1, 15, 60, 200,
"e8dc63dcc641f32406dc4e8fb84918d9", "";
WebUsers 1 = "User",
"$1$4oCA0NXW0YuK3tiI297ZwZOTkZLCwsXKnZiezsTLyJA20jUxMWM/MTE6ODw4a2x1dXQndnchd
X0ueyp/eX19RUA=", 1, 0, 5, -1, 15, 60, 50,
"745000ce182823aea635d7017e610170", "";
```

[\WebUsers]

[TLSContexts]

```
FORMAT Index = Name, TLSVersion, DTLSVersion, ServerCipherString,
ClientCipherString, RequireStrictCert, TlsRenegotiation, OcspeEnable,
OcspeServerPrimary, OcspeServerSecondary, OcspeServerPort, OcspeDefaultResponse,
DHKeySize;
TLSContexts 0 = "default", 7, 0, "DEFAULT", "DEFAULT", 0, 1, 0, , , 2560, 0,
1024;
TLSContexts 1 = "audiocodes1288", 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]

[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,
SBCRTPMode, SBCJitterCompensation, SBCRemoteRenegotiateOnFaxDetection,
JitterBufMaxDelay, SBCUserBehindUdpNATRegistrationTime,
SBCUserBehindTcpNATRegistrationTime, SBCSDPHandlerRTCPAttribute,
SBCRemoveCryptoLifetimeInSDP, SBCIceMode, SBCRTPMux, SBCMediaSecurityMethod,
SBCHandleXDetect, SBCRTPFeedback, 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 = "Session_Manager", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24,
0, 0, 0, 0, 0, 0, 1, -1, 1, 0, 1, -1, 1, 4, -1, 1, 1, 0, 0, "", "", 0, 0, "",
"", "", 0, 0, 0, 0, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0, 2, 2,
1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "",
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, -1, 0, 0, 0, 0, 1, 2, 0;

```

[\IpProfile]

[CpMediaRealm]

```

FORMAT Index = MediaRealmName, IPv4IF, IPv6IF, RemoteIPv4IF, RemoteIPv6IF,
PortRangeStart, MediaSessionLeg, PortRangeEnd, TCPPortRangeStart,
TCPPortRangeEnd, IsDefault, QoeProfile, BWProfile, TopologyLocation;
CpMediaRealm 0 = "DefaultRealm", "mp1288.avaya.com", "", "", "", 6000, 5953,
65529, 0, 0, 1, "", "", 0;

```

[\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]

[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 = "SIPInterface_0", "mp1288.avaya.com", "", 0, 0, 0, 5061, 0,
"", 0, "DefaultSRD", "", "audiocodes1288", -1, 0, 500, -1, 0, "", 0, -1, -1,
-1, 0, 0, "", "", -1;
```

[\SIPInterface]

[ProxySet]

```
FORMAT Index = ProxyName, EnableProxyKeepAlive, ProxyKeepAliveTime,
ProxyLoadBalancingMethod, IsProxyHotSwap, SRDName, ClassificationInput,
TLSContextName, ProxyRedundancyMode, DNSResolveMethod, KeepAliveFailureResp,
GWIPv4SIPInterfaceName, SBCIPv4SIPInterfaceName, GWIPv6SIPInterfaceName,
SBCIPv6SIPInterfaceName, MinActiveServersLB, SuccessDetectionRetries,
SuccessDetectionInterval, FailureDetectionRetransmissions;
ProxySet 0 = "ProxySet_0", 0, 60, 0, 0, "DefaultSRD", 0, "audiocodes1288", -
1, -1, "", "SIPInterface_0", "", "", "", 1, 1, 10, -1;
```

[\ProxySet]

[IPGroup]

```
FORMAT Index = Type, Name, ProxySetName, VoiceAConnector, SIPGroupName,
ContactUser, SipReRoutingMode, AlwaysUseRouteTable, SRDName, MediaRealm,
InternalMediaRealm, ClassifyByProxySet, ProfileName, MaxNumOfRegUsers,
InboundManSet, OutboundManSet, RegistrationMode, AuthenticationMode,
MethodList, SBCServerAuthType, OAuthHTTPService, EnableSBCClientForking,
SourceUriInput, DestUriInput, ContactName, Username, Password, UIFormat,
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, "Default_IPG", "ProxySet_0", "", "avaya.com", "", -1, 0,
"DefaultSRD", "DefaultRealm", "DefaultRealm", 0, "Session_Manager", -1, -1, -
1, 0, 0, "", -1, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", 0, "", "", 0,
0, "audiocodes1288", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0, "", 1, "", 0, 0,
"";
```

[\IPGroup]

[PREFIX]

FORMAT Index = RouteName, DestinationPrefix, DestAddress, SourcePrefix, ProfileName, MeteringCodeName, DestPort, DestIPGroupName, TransportType, SrcTrunkGroupId, DestSIPInterfaceName, CostGroup, ForkingGroup, CallSetupRulesSetId, DestTags, SrcTags;
PREFIX 0 = "Tel to Ip", "*", "10.64.110.212", "*", "", "", 5061, "", 2, 1, "SIPInterface_0", "", -1, -1, "", "";

[\PREFIX]

[TrunkGroup]

FORMAT Index = TrunkGroupNum, FirstTrunkId, FirstBChannel, LastBChannel, FirstPhoneNumber, ProfileName, LastTrunkId, Module;
TrunkGroup 0 = 1, 255, 1, 1, "70111", "", 255, 1;
TrunkGroup 1 = 1, 255, 2, 2, "70112", "", 255, 1;

[\TrunkGroup]

[PstnPrefix]

FORMAT Index = RouteName, DestPrefix, TrunkGroupId, SourcePrefix, SourceAddress, ProfileName, SrcIPGroupName, DestHostPrefix, SrcHostPrefix, SrcSIPInterfaceName, TrunkId, CallSetupRulesSetId, DestType, DestTags, SrcTags;
PstnPrefix 0 = "IP to Tel", "*", 1, "*", "*", "", "", "*", "*", "SIPInterface_0", -1, -1, 0, "", "";

[\PstnPrefix]

[ProxyIp]

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

[\ProxyIp]

[TrunkGroupSettings]

FORMAT Index = TrunkGroupId, ChannelSelectMode, RegistrationMode, GatewayName, ContactUser, ServingIPGroupName, MWIInterrogationType, TrunkGroupName, UsedByRoutingServer, AdminState, DedicatedConnectionMode;
TrunkGroupSettings 0 = 1, 0, 0, "", "", "Default_IPG", 255, "TrunkGroup-1", 0, 0, 0;

[\TrunkGroupSettings]

[Authentication]

FORMAT Index = UserId, UserPassword, Module, Port, PortType;
Authentication 0 = "70111", "\$1\$tIWHhYONjw==", 1, 1, "FXS";
Authentication 1 = "70112", "\$1\$tIWHhYONjw==", 1, 2, "FXS";

[\Authentication]

[GwRoutingPolicy]

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

[\GwRoutingPolicy]

[ResourcePriorityNetworkDomains]

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

[\ResourcePriorityNetworkDomains]

[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]

©2020 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.