



Avaya Solution & Interoperability Test Lab

Application Notes for AudioCodes Mediant 500Li Analog Gateway with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise – Issue 1.0

Abstract

These Application Notes contain instructions for configuring AudioCodes Mediant 500Li Analog Gateway R7.20AN in the Avaya enterprise and outside the enterprise in a remote worker configuration. The enterprise environment incorporates Avaya Session Border Controller for Enterprise 8.1, Avaya Aura® Communication Manager 8.1, and Avaya Aura® Session Manager 8.1. Compliance testing was conducted to verify interoperability. The AudioCodes Mediant 500Li GE/GE/8FXS 8 Port FXS Analog Gateway was used for testing.

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.

Table of Contents

Table of Contents	2
1. Introduction	5
2. General Test Approach and Test Results	5
2.1. Interoperability Compliance Testing	6
2.2. Test Results	6
2.3. Support	6
3. Reference Configuration	7
4. Equipment and Software Validated	8
5. Configure Avaya Aura® Communication Manager	9
5.1. Verify Avaya Aura® Communication Manager License	9
5.2. Administer IP Network Region	11
5.2.1. IP Network Region for Voice and Fax Calls	11
5.3. Administer IP Codec Set	12
5.3.1. IP Codec set for Voice and Fax Calls	12
5.4. Administer IP Node Names	13
5.5. Administer SIP Signaling Group	14
5.5.1. Signaling Group for Voice and Fax Calls	14
5.6. Administer SIP Trunk Group	15
5.6.1. Trunk Group for Voice and Fax Calls	15
5.7. Administer Route Pattern	16
5.8. Administer Private Numbering	17
5.9. Administer AAR Analysis	17
6. Configure Avaya Aura® Session Manager	18
6.1. Add SIP Domain	19
6.2. Add Location	20
6.3. Add Adaptations	21
6.4. Add SIP Entities	22
6.4.1. Communication Manager	22
6.4.2. Avaya Session Border Controller for Enterprise	23
6.5. Add Entity Links	24
6.5.1. Communication Manager	24
6.5.2. Session Border Controller for Enterprise	25
6.6. Add Routing Policy	26
6.7. Add Dial Patterns	27
6.8. Add Users	28
6.8.1. Identity	28
6.8.2. Communication Address	29
6.8.3. Communication Profile	30
6.8.4. Session Manager Profile	31
6.8.5. CM Endpoint Profile	32
7. Administer Session Border Controller for Enterprise	33
7.1. Launch SBCE Web Interface	34
7.2. Administer Network Management	35

7.3.	Administer TLS Profiles	36
7.3.1.	Configure Avaya SBCE TLS Client Profiles	37
7.3.2.	Configure Avaya SBCE TLS Server Profiles	39
7.4.	Administer SIP Servers.....	41
7.4.1.	SIP Server for Session Manager.....	41
7.4.2.	SIP Server for VoIPSP	42
7.5.	Administer Routing Profiles	43
7.5.1.	Routing Profile for Session Manager	43
7.5.2.	Routing Profile for VoIPSP.....	44
7.6.	Administer Media Rules	45
7.7.	Administer End Point Policy Groups	46
7.8.	Administer Media Interfaces	47
7.9.	Administer Signaling Interfaces	48
7.10.	Administer End Point Flows	48
7.10.1.	Remote Worker Subscriber Flow	49
7.10.2.	Session Manager Server Flows	51
7.10.3.	VoIPSP Server Flows.....	53
8.	Configure AudioCodes Mediant 500Li	54
8.1.	Initial Network Setup.....	54
8.1.1.	Assumptions	54
8.1.2.	Changes to the configuration example below	55
8.1.3.	CLI Configuration	55
8.2.	Verify/Upgrade Firmware Version.....	57
8.3.	Set System Time and Date.....	58
8.4.	Administer Syslog Settings.....	59
8.5.	Administer Security	60
8.5.1.	TLS Contexts.....	60
8.5.2.	Administer Security Settings.....	61
8.6.	Administer Media	62
8.6.1.	Administer Media Security	62
8.6.2.	Install Certificates	63
8.6.3.	Administer Media Settings.....	65
8.7.	Administer SIP Definitions.....	66
8.7.1.	General settings	66
8.7.2.	Transport Settings	67
8.7.3.	Proxy Registration.....	68
8.7.4.	Administer Call Detail Records	69
8.8.	Administer Coder Groups.....	70
8.8.1.	Administer Tel Profiles	71
8.9.	Configure Core Administration	72
8.9.1.	Media Realm	72
8.9.2.	SIP Interface	73
8.9.3.	Proxy Set	74
8.9.4.	IP Groups.....	76
8.10.	Administer Gateway	77
8.10.1.	Trunk Groups	77

8.10.2.	Trunk Group Settings	78
8.10.3.	Tel-to-IP Routing	79
8.10.4.	IP-to-Tel Routing	80
8.10.5.	Authentication	81
8.10.6.	Gateway General Settings	82
8.10.7.	Supplementary Services Settings	83
9.	Verification Steps.....	84
9.1.	Avaya Aura® Communication Manager and Avaya Aura® Session Manager	84
9.2.	Avaya Session Border Controller for Enterprise	86
9.3.	AudioCodes Mediant 500Li	87
10.	Conclusion	89
11.	Additional References	89

1. Introduction

The AudioCodes Mediant 500Li Analog Gateway (Mediant 500Li) implements voice technology that connects analog telephones and fax machines to IP-based enterprise PBX systems. In the compliance test, AudioCodes Mediant 500Li provided SIP access to analog devices to verify interoperability within an enterprise Avaya Aura® IP Telephony Environment. AudioCodes Mediant 500Li registers to Avaya Aura® Session Manager when located within the enterprise. AudioCodes Mediant 500Li registers to Avaya Aura® Session Manager through Avaya Session Border Controller for Enterprise (SBCE) when located outside the enterprise as a Remote Worker. The AudioCodes Mediant 500Li GE/GE/8FXS 8 Port FXS Analog Gateway was used for testing.

2. General Test Approach and Test Results

Interoperability compliance testing focused on verifying various inbound and outbound call flows between AudioCodes Mediant 500Li, Communication Manager, Session Manager, and Session Border Controller for Enterprise

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and AudioCodes Mediant 500Li employed TLS connectivity with SRTP.

2.1. Interoperability Compliance Testing

AudioCodes Mediant 500Li registered analog lines as SIP users on Session Manager. AudioCodes Mediant 500Li registered analog lines as SIP users to Session Manager through Avaya Session Border Controller for Enterprise as a Remote Worker. SIP, TLS, and SRTP were utilized during this test effort. Note that compliance testing only verified the analog lines provided by the gateway and no other features on Mediant 500Li. The following analog line features and functionalities were covered during compliance testing:

- Incoming calls from Avaya SIP/H.323 endpoints and PSTN to AudioCodes Mediant 500Li (with the Mediant 500Li located in the enterprise as well as in a remote worker location)
- Outgoing calls from AudioCodes Mediant 500Li to Avaya SIP/H.323 endpoints and PSTN (with the Mediant 500Li located in the enterprise as well as in a remote worker location)
- SIP signaling using TLS
- Voice codecs G.711U, G.711A and G.729AB using SRTP
- Incoming and outgoing faxes using encrypted G.711 (in pass-through mode)
- DTMF tone transmission with RFC2833
- Calls using various Avaya endpoints, including analog, digital, H.323, and SIP
- Basic features including Hold/Resume, DTMF transmission, Voicemail with Message Waiting Indicator (MWI)

2.2. Test Results

All test cases passed. The following observations were noted during the compliance testing:

- Mediant 500Li does not support encrypted T.38 FAX. Testing verified encrypted G.711 Fax in pass-through mode.
- TLS/SRTP testing employed a mandatory media encryption configuration. Mediant 500Li does not currently support attribute capability negotiation as defined in RFC5939. To use Mediant 500Li preferable media encryption, message manipulations would have to be configured to remove the acap: attribute from the SRTP line.
- Voicemail MWI was verified using stutter tone message waiting notification.

2.3. Support

Technical support for AudioCodes Mediant 500Li Analog Gateway 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

AudioCodes Mediant 500Li is shown below in the Enterprise or configured as Remote Worker.

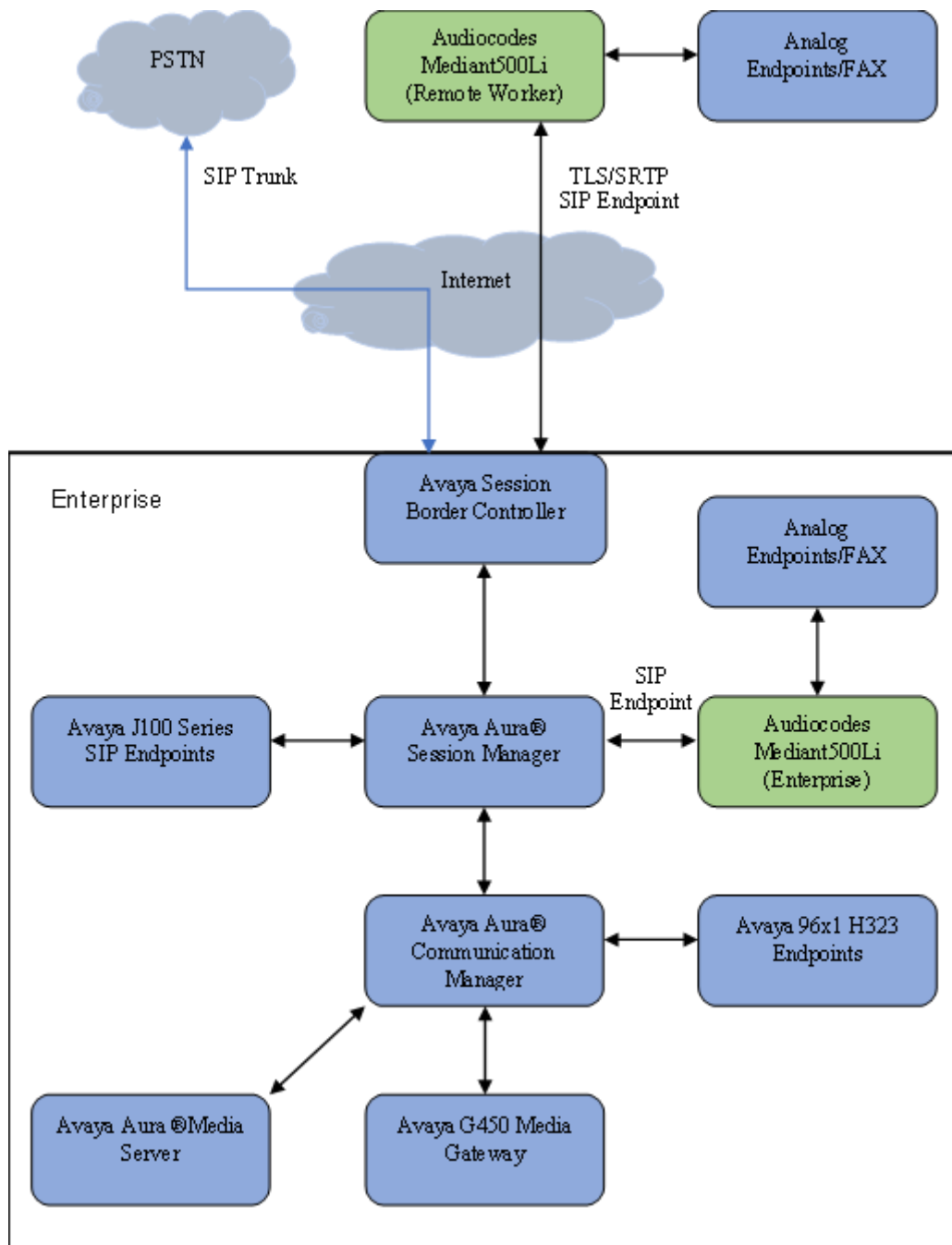


Figure 1: AudioCodes Mediant 500Li Analog Gateway Configuration

4. Equipment and Software Validated

The following equipment and software were used for interoperability testing:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Virtual Machine	8.1.3.0.1.890.26685
Avaya Aura® Session Manager running on Virtual Machine	8.1.3.0.813014
Avaya Aura® System Manager running on Virtual Machine	8.1.3.0.813014
Avaya Session Border Controller for Enterprise running on Virtual Machine	8.1.2.0-19809
Avaya G450 Media Gateway	41.34.1
Avaya Aura® Media Server	8.0.2.163
Avaya 1408 Digital Phone	NA
Avaya 6220 Analog Phone	NA
Avaya 9641G H.323 Deskphone	6.8.3.04
Avaya J179 SIP Deskphone	4.0.9.0.4
AudioCodes Mediant 500Li Analog Gateway	7.20AN.456.539

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 1**, verify that the number of OPS stations allowed in the system is sufficient for the number of Mediant 500Li analog lines (as SIP endpoints) that will be deployed.

```
display system-parameters customer-options                               Page 1 of 12
                                OPTIONAL FEATURES

G3 Version: V18                                     Software Package: Enterprise
Location: 2                                           System ID (SID): 1
Platform: 28                                         Module ID (MID): 1

                                USED
Platform Maximum Ports: 48000      111
Maximum Stations: 36000            86
Maximum XMOBILE Stations: 36000    0
Maximum Off-PBX Telephones - EC500: 41000    0
Maximum Off-PBX Telephones - OPS: 41000    51
Maximum Off-PBX Telephones - PBFMC: 41000    0
Maximum Off-PBX Telephones - PVFMC: 41000    0
Maximum Off-PBX Telephones - SCCAN: 0        0
Maximum Survivable Processors: 313    0

(NOTE: You must logoff & login to effect the permission changes.)
```

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	6
Maximum Administered Remote Office Trunks:	12000	0
Maximum 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	2
Maximum Video Capable IP Softphones:	2400	23
Maximum Administered SIP Trunks:	12000	10
Maximum Administered Ad-hoc Video Conferencing Ports:	12000	0
Maximum Number of DS1 Boards with Echo Cancellation:	688	0
(NOTE: You must logoff & login to effect the permission changes.)		

On **Page 5**, verify **Media Encryption Over IP** is 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	
(NOTE: You must logoff & login to effect the permission changes.)	

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.

5.2.1. IP Network Region for Voice and Fax Calls

Configure this network region as follows:

- Set **Name** to an appropriate value
- Set **Location** to **1**
- Set **Codec Set** to that administered in **Section 5.3**, e.g., **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? n
        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
        Keep-Alive Count: 5
```

5.3. Administer IP Codec Set

Use the **change ip-codec-set *n*** command to configure IP codec set, where *n* is the codec set used in **Section 5.2.1** IP Network Region administration.

5.3.1. IP Codec set for Voice and Fax Calls

Configure this codec set as follows, on **Page 1**:

- Set **Audio Codec 1, 2 and 3** to **G.711MU**, **G.711A**, **G.729AB** respectively
- Set **Media Encryption 1:** to **1-srtp-aescm128-hmac80** and **Media Encryption 2:** to **2-srtp-aescm128-hmac32**
- Set **Encrypted SRTCP** to **enforce-unenc-srtp**

Note: G.711MU, G.711A and G.729AB codecs were used 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: G.729AB     n           2          20
4:
5:
6:
7:

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

On **Page 2**:

FAX settings allow the use of encrypted G.711 Fax Mode. Encrypted T.38 is not supported as noted in **Section 2.2**.

- Set **FAX Mode** to **pass-through**

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

                                IP MEDIA PARAMETERS

                                Allow Direct-IP Multimedia? y
                                Maximum Call Rate for Direct-IP Multimedia: 10240:Kbits
                                Maximum Call Rate for Priority Direct-IP Multimedia: 10240:Kbits

FAX      Mode      Redundancy      Packet
          pass-through      0      ECM: y
Modem      off      0
TDD/TTY      US      3
H.323 Clear-channel      n      0
SIP 64K Data      n      0      20
```

5.4. Administer IP Node Names

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

```
change node-names ip
```

Name	IP Address
aes81	10.64.110.215
aes811	10.64.110.209
ams81	10.64.110.214
aura_cms18	10.64.110.20
cms19	10.64.110.225
default	0.0.0.0
procr	10.64.110.213
procr6	::
remotecms191	10.64.110.226
sm81	10.64.110.212

(10 of 10 administered node-names were displayed)
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name

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.

5.5.1. Signaling Group for Voice and Fax Calls

Configure this signaling group as follows:

- Set **Group Type** to **sip**
- Set **Transport Method** to **tls**
- Set **Near-end Node Name** to **procr**
- Set **Near-end Listen Port** to **5061**
- Set **Far-end Node Name** to the configured Session Manager name in **Section 5.4** e.g., **sm81**
- Set **Far-end Listen Port** to **5061**
- Set **Far-end Network region** to the configured IP network region in **Section 5.2.1** e.g., **1**
- Enter a **Far-end Domain**, e.g., **avaya.com**
- Set **Direct IP-IP Audio Connections** to **y**
- Set **Initial IP-IP Direct Media** to **y**
- Set **DTMF over IP** to **rtp-payload**

Communication Manager supports DTMF transmission using RFC 2833.

```
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? y                      Priority 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: avaya.com

Incoming Dialog Loopbacks: eliminate          Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload                    RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 65          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? y
                                           Alternate Route Timer(sec): 6
```

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.

5.6.1. Trunk Group for Voice and Fax Calls

Configure this trunk group as follows, on **Page 1**:

- Set **Group Type** to **sip**
- Enter an appropriate **Group Name** e.g., **SM Trunk 1**
- Enter a valid **TAC** e.g., **101**
- Set **Service Type** to **tie**
- Enter **Signaling Group** value to the signaling group configured in **Section 5.5.1** e.g., **1**
- Enter a desired number in **Number of Members** field

```
change trunk-group 1                                     Page 1 of 5

                                TRUNK GROUP

Group Number: 1                      Group Type: sip          CDR Reports: y
  Group Name: SM Trunk 1              COR: 1                TN: 1          TAC: 101
  Direction: two-way                  Outgoing Display? y
  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 **Numbering Format** to **private**

```
TRUNK FEATURES
  ACA Assignment? n                      Measured: both
                                          Maintenance Tests? y

  Suppress # Outpulsing? n  Numbering Format: private
                              UI Treatment: shared
                              Maximum Size of UI Contents: 128
                              Replace Restricted Numbers? n
                              Replace Unavailable Numbers? n

                              Modify Tandem Calling Number: no
  Send UCID? y

  Show ANSWERED BY on Display? y

  DSN Term? n                      Hold/Unhold
```

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 an appropriate name in **Pattern Name** field
- For line 1, set **Grp No** to the trunk group configured in **Section 5.6.1** e.g., **1**
- For line 1, set **FRL** to **0**
- For line 1, set **Numbering Format** to **lev0-pvt**

change route-pattern 1													Page 1 of 3	
Pattern Number: 1													Pattern Name: main	
SCCAN? n		Secure SIP? y		Used for SIP stations? 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				
3:									n	user				
4:									n	user				
5:									n	user				
6:									n	user				
BCC VALUE		TSC	CA-TSC		ITC BCIE		Service/Feature		PARM	Sub	Numbering	LAR		
0 1 2 M 4 W			Request						Dgts	Format				
1:	y	y	y	y	y	n	n	rest			lev0-pvt	none		
2:	y	y	y	y	y	n	n	rest				none		
3:	y	y	y	y	y	n	n	rest				none		
4:	y	y	y	y	y	n	n	rest				none		
5:	y	y	y	y	y	n	n	rest				none		
6:	y	y	y	y	y	n	n	rest				none		

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. For compliance testing, 5-digit extensions beginning with 7 are 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		
5	5			5	Total Administered: 2	
5	7			5	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 both voice and fax calls.

- 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**, e.g., **1**
- Set **Call Type** to **lev0**

Note: The extension range used in this step needs an entry to the dial plan.

change aar analysis 7							
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

This section provides the procedures for configuring Session Manager. It is assumed that the basic configuration is already in place. This section discusses the following areas:

- Add SIP Domain
- Add Location
- Add Adaptations
- Add SIP Entities
- Add Entity Links
- Add Routing Policy
- Add Dial Patterns
- Add Users

Note: The sections that reference configuration related to the Avaya Session Border Controller for Enterprise are only needed if the Median500Li is located outside the enterprise environment and registering through the internet as remote workers.

Access Session Manager Administration web interface by entering **http://<ip-address>/SMGR** in a web browser, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials.



Recommended access to System Manager is via FQDN.

[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

Password:

[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

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 5.2.1**) e.g., **avaya.com**
- Set **Type** to **sip**

Click **Commit** to save changes.

The screenshot displays the Avaya Aura System Manager 8.1 interface for Domain Management. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and menus for 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are also visible. The main content area is titled 'Domain Management' and features 'Commit' and 'Cancel' buttons. Below the title is a table with one item, 'avaya.com', with a type of 'sip'. The 'Name' and 'Type' fields are highlighted with a red box. The table has columns for 'Name', 'Type', and 'Notes'. A 'Filter: Enable' button is located to the right of the table. The interface also includes a 'Help ?' link in the top right corner.

6.2. Add Location

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

Under **General**:

- Type in a descriptive **Name** e.g., **DevConnect**
- 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 shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also present. The main content area is titled 'Location Details' and includes a 'Commit' button and a 'Cancel' button. The 'General' section contains a red-bordered box around the '* Name: DevConnect' field, with a 'Notes:' field below it. The 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled:' checkbox and fields for 'Listed Directory Number' and 'Associated CM SIP Entity'. The 'Overall Managed Bandwidth' section includes a 'Managed Bandwidth Units' dropdown set to 'Kbit/sec', and fields for 'Total Bandwidth', 'Multimedia Bandwidth', and 'Audio Calls Can Take Multimedia Bandwidth' (checked). The 'Per-Call Bandwidth Parameters' section has fields for 'Maximum Multimedia Bandwidth (Intra-Location)' and 'Maximum Multimedia Bandwidth (Inter-Location)', both set to '2000 Kbit/Sec'.

6.3. Add Adaptations

Note: The configuration in this section is only needed if Mediant 500Li is located outside the enterprise environment and registering through the internet as remote workers.

Add an adaptation to convert incoming domains from an IP address to the pertinent domain. Select **Adaptations** → **Adaptations** from the left pane and click **New** (not shown) to add a new adaptation for IPC.

The **Adaptation Details** screen is displayed. Enter the following values for the specified fields:

- **Adaptation Name:** A descriptive name, e.g., **ASBCE812**.
- **Module Name:** **DigitConversionAdapter**
- **Module Parameter Type:** **Name-Value Parameter**

Click **Add** to add the adaptation name value pairs as specified:

- **fromto:** **true**
- **iodstd:** The pertinent domain name, e.g., **avaya.com**
- **iosrcd:** The pertinent domain name, e.g., **avaya.com**
- **odstd:** The pertinent domain name, e.g., **avaya.com** (not shown)
- **osrcd:** The pertinent domain name, e.g., **avaya.com** (not shown)

Click **Commit** to save changes.

The screenshot shows the 'Adaptation Details' screen in the AVAYA Aura System Manager 8.1. The interface includes a top navigation bar with 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts' menus, a search bar, and a user profile 'admin'. The main content area is titled 'Adaptation Details' and has 'Commit' and 'Cancel' buttons. The 'General' tab is active, showing the following fields:

- * Adaptation Name:** ASBCE812
- Notes:** (empty text area)
- * Module Name:** DigitConversionAdapter (dropdown menu)
- Type:** digit
- State:** enabled (dropdown menu)
- Module Parameter Type:** Name-Value Parameter (dropdown menu)

Below these fields is a table with columns 'Name' and 'Value'. The table contains three rows, each with a checkbox in the 'Name' column:

Name	Value
<input type="checkbox"/> fromto	true
<input type="checkbox"/> iodstd	avaya.com
<input type="checkbox"/> iosrcd	avaya.com

The table is highlighted with a red box. Below the table is a 'Select' dropdown menu set to 'All, None' and a pagination bar showing 'Page 1 of 2'. At the bottom of the screen, there is an 'Egress URI Parameters' text area.

NOTE: SIP message manipulation to modify the incoming domain can be done through AudioCodes administration. Interoperability testing employed this adaptation too.

6.4. Add SIP Entities

Add a SIP entity for Communication Manager and for Session Border Controller for Enterprise.

6.4.1. Communication Manager

Add Communication Manager as a SIP Entity. Navigate to **Elements → Routing → SIP Entities**, click on **New** (not shown) and configure as follows:

- Type in a descriptive name in **Name** field, e.g., **cm81**
- Type in the IP address or FQDN of Communication Manager in **FQDN or IP Address** field, e.g., **10.64.110.213**
- Set **Type** to **CM**
- Set **Location** to the location configured in **Section 6.2**, e.g., **DevConnect**

Click **Commit** to save changes.

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

AVAYA Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ admin

Home Routing

R...

SIP Entity Details

Commit Cancel

General

* Name: cm81

* FQDN or IP Address: 10.64.110.213

Type: CM ▾

Notes:

Adaptation: ▾

Location: DevConnect ▾

Time Zone: America/Denver ▾

* SIP Timer B/F (in seconds): 4

Minimum TLS Version: Use Global Setting ▾

Credential name:

Securable: ☐

Call Detail Recording: none ▾

Loop Detection

Loop Detection Mode: On ▾

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

Monitoring

SIP Link Monitoring: Use Session Manager Configuration ▾

Help ?

6.4.2. Avaya Session Border Controller for Enterprise

Note: The configuration in this section is only needed if Mediant 500Li is located outside the enterprise environment and registering through the internet.

Add Session Border Controller as a SIP Entity. Navigate to **Elements** → **Routing** → **SIP Entities**, click on **New** (not shown) and configure as follows:

- Type in a descriptive name in **Name** field, e.g., **ASBCE812**
- Type in the IP address of the internal SBCE Interface from **Section 7.2** in **FQDN or IP Address** field, e.g., **10.64.110.242**
- Set **Type** to **SIP Trunk**
- Set **Location** to the location configured in **Section 6.2**

Click **Commit** to save changes.

AVAYA Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ | admin

Home Routing

R...

SIP Entity Details Commit Cancel Help ?

General

* Name: ASBCE812

* FQDN or IP Address: 10.64.110.242

Type: SIP Trunk ▾

Notes:

Adaptation: ▾

Location: DevConnect ▾

Time Zone: America/Denver ▾

* SIP Timer B/F (in seconds): 4

Minimum TLS Version: Use Global Setting ▾

Credential name:

Securable: ☐

Call Detail Recording: egress ▾

Loop Detection

Loop Detection Mode: On ▾

6.5. Add Entity Links

Add entity links between Communication Manager and Session Manager and between SBCE and Session Manager.

6.5.1. Communication Manager

Add an entity link between Communication Manager and Session Manager. 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 e.g., **sm81**
- Set **SIP Entity 2** to Communication Manager SIP Entity configured in **Section 6.4.1** e.g., **cm81**
- Set **Protocol** to **TLS**
- Set **Port** to **5061**

Click **Commit** to save changes.

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ admin

Home Routing

R...

Entity Links Commit Cancel [Help ?](#)

1 Item [Refresh](#) Filter: Enable

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

Select : All, None

Commit Cancel

6.5.2. Session Border Controller for Enterprise

Note: The configuration in this section is only needed if Mediant 500Li is located outside the enterprise environment and registering through the internet as remote workers.

Add an Entity link between SBCE and Session Manager. 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 Session Manager Entity name e.g., **sm81**
- Set **SIP Entity 2** to the SBCE SIP Entity name from **Section 6.4.2** e.g., **ASBCE812**
- Set **Protocol** to **TLS**
- Set **Port** to **5061**

Click **Commit** to save changes.

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 admin

Home Routing

Entity Links Commit Cancel [Help ?](#)

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	P
<input type="checkbox"/>	* sm81_SBCE812_5061_TL	* sm81	TLS ▾	* 5061	* ASBCE812	

Select : All, None

Commit Cancel

6.6. Add Routing Policy

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. 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 6.4.1** e.g., **cm81**

Click **Commit** to save changes.

AVAYA Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ | admin

Home Routing

R...

Routing Policy Details Commit Cancel [Help ?](#)

General

* **Name:**

Disabled: ☐

* **Retries:**

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
cm81	10.64.110.213	CM	

Time of Day

Add Remove View Gaps/Overlaps

1 Item [Refresh](#) Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

6.7. Add Dial Patterns

Dial patterns are defined to direct calls to the appropriate SIP Entity. Navigate to **Elements** → **Routing** → **Dial Patterns**, click on **New** (not shown) and configure as follows:

Under **General**:

- Set **Pattern** to prefix of dialed number e.g., **70**
- Set **Min** to minimum length of dialed number e.g., **5**
- Set **Max** to maximum length of dialed number e.g., **5**

Under **Originating Locations and Routing Policies**:

- Click **Add** and select the location configured in **Section 6.2** for **Originating Location**. Interoperability testing used **-ALL-** in this case
- Select the Communication Manager routing policy administered in **Section 6.6** for **Routing Policies** e.g., **cm81**

Click **Commit** to save changes.

AVAYA Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 admin

Home Routing

R...

Dial Pattern Details Commit Cancel

General

* **Pattern:** 70

* **Min:** 5

* **Max:** 5

Emergency Call: ☐

SIP Domain: avaya.com ▾

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

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

Select : All, None

6.8. Add Users

For each analog line on AudioCodes Mediant 500Li, a user needs to be added on Session Manager. Information in this section will be used by AudioCodes Mediant 500Li for registering to Session Manager.

Navigate to **Users → User Management → Manage Users** to display the **User Management** screen (not shown). Click + **New** to add a user.

6.8.1. Identity

Enter values for the following required attributes for a new SIP user in the **New User Profile** screen:

- Enter appropriate name for **Last Name**, e.g., **AudioCodes**
- Enter appropriate name for **First Name**, e.g., **User 1**
- Enter <extension>@<sip domain> for the **Login Name**, e.g., **70111@avaya.com**)

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The main content area is titled 'User Profile | Edit | 70111@avaya.com'. The 'Basic Info' tab is active, showing fields for 'Last Name', 'First Name', 'Login Name', 'Address', 'LocalizedName', 'User Provisioning Rule', 'Description', 'Password', 'Confirm Password', 'Endpoint Display Name', 'Last Name (in Latin alphabet characters)', 'First Name (in Latin alphabet characters)', 'Middle Name', 'Email Address', 'User Type', 'Localized Display Name', and 'Title Of User'. A red box highlights the 'Last Name', 'First Name', and 'Login Name' fields, which are marked as required with an asterisk. The values entered are 'AudioCodes', 'User 1', and '70111@avaya.com' respectively.

Press **Commit & Continue** after making entries or selections.

6.8.2. Communication Address

Select **Communication Address** in the left list and click + **New** (not shown).

Enter the following attributes for the **Communication Address**:

- Select **Avaya SIP** from the drop-down list for **Type**
- Enter the extension number for **Fully Qualified Address**, e.g., **70111**
- Enter the **domain** (e.g., **avaya.com**)

Click **OK**.

The screenshot displays the Avaya Aura System Manager 8.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and tabs for 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are also visible. The main content area is titled 'User Profile | Edit | 70111@avaya.com' and includes tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, showing a list of profiles with toggle switches. A modal dialog box titled 'Communication Address Add/Edit' is open in the foreground. It contains two fields: '* Type:' with a dropdown menu set to 'Avaya SIP', and '*Fully Qualified Address:' with a text input containing '70111' and a dropdown menu set to 'avaya.com'. The dialog box has 'Cancel' and 'OK' buttons at the bottom right.

6.8.3. Communication Profile

Click the **Communication Profile** tab and in the **Comm-Profile Password** and **Re-enter Comm-Profile Password** fields, enter a numeric password. This will be used to register the device during login. Click **OK**.

The screenshot displays the Avaya Aura System Manager 8.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and tabs for 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are also visible. The main content area shows the 'User Profile | Edit | 70111@avaya.com' page. The 'Communication Profile' tab is selected. A modal dialog titled 'Comm-Profile Password' is open, containing two password input fields: 'Comm-Profile Password' and 'Re-enter Comm-Profile Password'. Below the fields is a link 'Generate Comm-Profile Password' and buttons for 'Cancel' and 'OK'. The background shows the user profile details and a list of profiles.

6.8.4. Session Manager Profile

Click on the **Session Manager Profile** slide button. For **Primary Session Manager**, **Origination Sequence**, **Termination Sequence**, and **Home Location** (not shown), select the values corresponding to the applicable Session Manager and Communication Manager application sequences. Retain the default values in the remaining fields.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and various menu items like 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are also visible. The main content area is titled 'User Profile | Edit | 70111@avaya.com' and features tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, showing a 'Communication Profile Password' section and a 'PROFILES' list. In the 'PROFILES' list, 'Session Manager Profile' is selected and toggled on. The 'SIP Registration' section contains fields for 'Primary Session Manager' (set to 'sm81'), 'Secondary Session Manager' (set to 'Start typing...'), 'Survivability Server' (set to 'Start typing...'), and 'Max. Simultaneous Devices' (set to '1'). There is also a checkbox for 'Block New Registration When Maximum Registrations Active?'. The 'Application Sequences' section, highlighted with a red box, shows 'Origination Sequence' and 'Termination Sequence' both set to 'cm81'.

6.8.5. CM Endpoint Profile

Click on the **CM Endpoint Profile** slide button. Fill in the following fields:

- Select the relevant Communication Manager SIP Entity for **System** e.g., **cm81**
- Select **Endpoint** for **Profile Type**
- Select **J179_DEFAULT_CM_8_1** for **Template**
- Enter the **Extension** number (e.g., **70111**)

Click on **Endpoint Editor** in the Extension field to edit Communication Manager settings. Input the appropriate **coverage path 1** number(not shown) to route unanswered calls to voicemail. Click **Done** to close the Endpoint Editor. Click **Commit**.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, a search bar, and user information (admin). The main navigation menu on the left shows 'Home', 'User Management', and 'Routing'. The 'User Management' section is expanded, showing 'Users' and 'Manage Users'. The 'User Profile | Edit | 70111@avaya.com' page is open, with the 'Communication Profile' tab selected. The left sidebar shows the 'CM Endpoint Profile' selected. The main form area contains the following fields and options:

- System:** cm81 (highlighted with a red box)
- Profile Type:** Endpoint (highlighted with a red box)
- Extension:** 70111 (highlighted with a red box)
- Template:** J179_DEFAULT_CM_8_1 (highlighted with a red box)
- Set Type:** J179
- Security Code:** Enter Security Code
- Voice Mail Number:** (empty field)
- Preferred Handle:** Select
- SIP URI:** Select
- Calculate Route Pattern:** ☒
- Delete on Unassign from User or on Delete User:** ☒
- Override Endpoint Name and Localized Name:** ☒
- Allow H.323 and SIP Endpoint Dual Registration:** ☐

7. Administer Session Border Controller for Enterprise

SBCE provides an edge capability to allow remote worker registration external to the private enterprise network. Remote workers interact with the external interface of SBCE while the SBCE internal interface is shielded from the public external interface.

Note: The configuration in this section is only needed if the Median500Li is located outside the enterprise environment and registering through the internet.

The configuration steps on SBCE include the following:

- Launch SBCE web interface
- Administer Network Management
- Administer Server TLS Profiles
- Administer SIP Servers
- Administer Routing Profiles
- Administer Media Rules
- Administer End Point Policy Groups
- Administer Media Interfaces
- Administer Signaling Interfaces
- Administer End Point Flows

The SBCE administration tasks will either be stepped through or displayed as administered.

7.1. Launch SBCE Web Interface

Access the SBCE web interface by using the URL **https://<ip-address>/sbc** in an Internet browser window, where **<ip-address>** is the IP address of the SBCE management interface. The screen below is displayed. Log in using the appropriate credentials.



Log In

Username:

[Continue](#)

Session Border Controller for Enterprise

WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2020 Avaya Inc. All rights reserved.

After logging in, the Dashboard will appear as shown below. All configuration screens of the SBCE are accessed by navigating the menu tree in the left pane. Select **Device** → **SBCE** from the top menu.

Device: EMS ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

EMS Dashboard

- Software Management
- Device Management
 - System Administration
 - Templates
- Backup/Restore
- Monitoring & Logging

Dashboard

Information	
System Time	01:37:28 PM MDT Refresh
Version	8.1.2.0-31-19809
GUI Version	8.1.2.0-19794
Build Date	Tue Dec 08 09:11:07 UTC 2020
License State	✔ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	09/09/2021 11:41:00 MDT
Failed Login Attempts	0

Active Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

None found.

[Add](#)

Notes

No notes found.

7.2. Administer Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the SBCE installation process, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency. Navigate to **Networks & Flows** → **Network Management**. On the Networks tab, select **Add** to add a new interface entry, or **Edit** to add or change IP addresses on an existing interface. The following screen shows the enterprise interface assigned to **A1** and the interface towards the Remote Workers assigned to **B1**.

Device: SBCE812 ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

Network Management

Media Interface

Signaling Interface

End Point Flows

Session Flows

Advanced Options

▸ DMZ Services

▸ Monitoring & Logging

Network Management

Interfaces

Networks

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
Internal-A1	10.64.110.1	255.255.255.0	A1	10.64.110.242, 10.64.110.243	Edit Delete
External-B1	10.64.102.1	255.255.255.0	B1	10.64.102.242, 10.64.102.243	Edit Delete

The following IP addresses and associated interfaces are used for remote workers in the reference configuration:

- 10.64.110.243: IP Address of Internal Interface A1 (Remote Workers media traffic)
- 10.64.102.243: IP Address of External Interface B1 (Remote Workers media traffic)

The IP address of 10.64.102.243 assigned to the external interface B1 is used for remote worker proxy registration. Click on the **Interfaces** tab (not shown) and verify the A1 and B1 interfaces are enabled. To enable an interface, click the corresponding **Disabled** link under the Status column to change it to **Enabled**.

7.3. Administer TLS Profiles

TLS profiles are created to assign identity certificates and CA certificates to SIP Servers. Certificate creation is not covered in these application notes. Details are provided in References [2] and [4] in **Section 11**. Both the internal and external interface SBCE identity certificates and their CA certificates should be installed in SBCE and available for use in TLS profiles.

7.3.1. Configure Avaya SBCE TLS Client Profiles

Select **TLS Management** → **Client Profiles** from the left-hand menu to create a SBCE TLS Client Profile. Click **Add**. Configure as follows:

- **Profile Name:** Input an appropriate name e.g., **ExternalClient**
- **Certificate:** Select the certificate for the external SBCE interface e.g., **sbceExternal.pem**
- **Peer Verification:** Set to **Required** by default
- **Peer Certificate Authorities:** Select the CA certificate e.g., **SMGRCA.pem**
- **Verification Depth:** Input **1**

Click **Next**. Accept default values for the next screen and click **Finish**. The default TLS version is **TLS 1.2**.

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

TLS Profile

Profile Name

ExternalClient

Certificate

sbceExternal.pem

SNI

☐ Enabled

Certificate Verification

Peer Verification

Required

Peer Certificate Authorities

AvayaDeviceEnrollmentCAchain.crt
avayaItrootca2.pem
entrust_g2_ca.cer
SMGRCA.pem

Peer Certificate Revocation Lists

Verification Depth

1

Extended Hostname Verification

☐

Server Hostname

Next

Create a SBCE TLS Client Profile for the internal SBCE interface. Configure as follows:

- **Profile Name:** Input an appropriate name e.g., **InternalClient**
- **Certificate:** Select the certificate for the internal SBCE interface e.g., **sbceInternal.pem**
- **Peer Verification:** Set to **Required** by default
- **Peer Certificate Authorities:** Select the CA certificate e.g., **SMGRCA.pem**
- **Verification Depth:** Input **1**

Click **Next**. Accept default values for the next screen and click **Finish**. The default TLS version is **TLS 1.2**.

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

TLS Profile

Profile Name

InternalClient

Certificate

sbceInternal.pem

SNI

☐ Enabled

Certificate Verification

Peer Verification

Required

Peer Certificate Authorities

AvayaDeviceEnrollmentCAchain.crt
avayaitrootca2.pem
entrust_g2_ca.cer
SMGRCA.pem

Peer Certificate Revocation Lists

Verification Depth

1

Extended Hostname Verification

☐

Server Hostname

Next

7.3.2. Configure Avaya SBCE TLS Server Profiles

Select **TLS Management** → **Server Profiles** from the left-hand menu to create an external SBCE TLS Server Profile. Click **Add**. Configure as follows:

- **Profile Name:** Input an appropriate name e.g., **External Server**
- **Certificate:** Select the certificate for the external SBCE interface e.g., **sbceExternal.pem**
- **Peer Verification:** Set to **None**

Click **Next**. Accept default values for the next screen and click **Finish**. The default TLS version is **TLS 1.2**.

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

TLS Profile	
Profile Name	ExternalServer
Certificate	sbceExternal.pem
SNI Options	None
SNI Group	None

Certificate Verification	
Peer Verification	None
Peer Certificate Authorities	AvayaDeviceEnrollmentCAchain.crt avayaaitrootca2.pem entrust_g2_ca.cer SMGRCA.pem
Peer Certificate Revocation Lists	
Verification Depth	0

Next

Select **TLS Management** → **Server Profiles** from the left-hand menu to create an internal SBCE TLS Server Profile. Click **Add**. Configure as follows:

- **Profile Name:** Input an appropriate name e.g., **InternalServer**
- **Certificate:** Select the certificate for the external SBCE interface e.g., **SBCEInternal.pem**
- **Peer Verification:** Set to **None**

Click **Next**. Accept default values for the next screen and click **Finish**. The default TLS version is **TLS 1.2**.

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

TLS Profile

Profile Name	<input type="text" value="InternalServer"/>
Certificate	<input type="text" value="sbceInternal.pem"/>
SNI Options	<input type="text" value="None"/>
SNI Group	<input type="text" value="None"/>

Certificate Verification

Peer Verification	<input type="text" value="None"/>
Peer Certificate Authorities	<div>AvayaDeviceEnrollmentCAchain.crt avayaitrootca2.pem entrust_g2_ca.cer SMGRCA.pem</div>
Peer Certificate Revocation Lists	<div></div>
Verification Depth	<input type="text" value="0"/>

7.4. Administer SIP Servers

A SIP server must be defined for each server in the SBCE environment.

Note: TLS profiles are defined in **Section 7.3**. Certificate generation is not covered in these application notes. Certificate installation steps for Mediant 500Li is shown in **Section 8.6.1**. All TLS certificates used for the compliance test were signed by System Manager.

7.4.1. SIP Server for Session Manager

To define a SIP server, navigate to **Services** → **SIP Servers** from the left pane to display the existing SIP server profiles. Click **Add** to create a new SIP server or select a pre-configured SIP server to view its settings. The **General** tab of the Session Manager SIP Server was configured as follows. TLS transport was used for the Session Manager SIP trunk. The TLS profile from **Section 7.3.1** was used. All other tabs were left with their default values.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes 'Device: SBCE812', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header shows 'Session Border Controller for Enterprise' and the 'AVAYA' logo.

The left sidebar contains the following menu items: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services (expanded), SIP Servers (selected), LDAP, RADIUS, Domain Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging.

The main content area is titled 'SIP Servers: SessionManager'. It features an 'Add' button and three action buttons: 'Rename', 'Clone', and 'Delete'. Below these are tabs for 'General', 'Authentication', 'Heartbeat', 'Registration', 'Ping', and 'Advanced'. The 'General' tab is active, showing the following configuration:

Server Type	Call Server	
TLS Client Profile	InternalClient	
DNS Query Type	NONE/A	
IP Address / FQDN	Port	Transport
10.64.110.212	5061	TLS

An 'Edit' button is located below the table.

7.4.2. SIP Server for VoIPSP

The **General** tab of the VoIPSP SIP Server is shown for illustrative purposes. The SIP server was configured as follows. UDP transport was used for the VoIPSP SIP trunk. All other tabs were left with their default values.

Device: SBCE812 ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
 SIP Servers
 LDAP
 RADIUS
▸ Domain Policies
▸ TLS Management
▸ Network & Flows
▸ DMZ Services
▸ Monitoring & Logging

SIP Servers: VoIPSP

Add

Rename Clone Delete

Server Profiles

VoIPSP

SessionManager

General

Authentication

Heartbeat

Registration

Ping

Advanced

Server Type

Call Server

DNS Query Type

NONE/A

IP Address / FQDN	Port	Transport
10.64.102.241	5060	UDP

Edit

RH: Reviewed
SPOC 11/22/2021

Solution & Interoperability Test Lab Application Notes
©2021 Avaya Inc. All Rights Reserved.

42 of 90
MD500LiRWCMSM81

7.5. Administer Routing Profiles

A routing profile defines where traffic will be directed. Administer a routing profile for Session Manager and the VoIPSP if needed.

7.5.1. Routing Profile for Session Manager

To create a new profile, navigate to **Configuration Profiles → Routing** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. To view the settings of an existing profile, select the profile from the center pane. The routing profile for calls to Session Manager is shown below. The routing profile was named **SessionManager**. This routing profile contains the IP address of the signaling interface of Session Manager.

Profile : SessionManager - Edit Rule

URI Group

*

Time of Day

default

Load Balancing

Priority

NAPTR

Transport

None

LDAP Routing

LDAP Server Profile

None

LDAP Base DN (Search)

None

Matched Attribute Priority

Alternate Routing

Next Hop Priority

Next Hop In-Dialog

Ignore Route Header

ENUM

ENUM Suffix

Add

Priority / Weight

LDAP Search Attribute

LDAP Search Regex Pattern

LDAP Search Regex Result

SIP Server Profile

Next Hop Address

Transport

1

Session!

10.64.110.212:

None

Delete

Finish

7.5.2. Routing Profile for VoIPSP

A routing profile for the VoIPSP trunk must exist. The routing profile for VoIPSP is shown below. This routing profile contains the IP address of the external SIP trunk interface of the VoIPSP Manager

Profile : VoIPSP - Edit Rule

URI Group

*

Time of Day

default

Load Balancing

Priority

NAPTR

Transport

None

LDAP Routing

LDAP Server Profile

None

LDAP Base DN (Search)

None

Matched Attribute Priority

Alternate Routing

Next Hop Priority

Next Hop In-Dialog

Ignore Route Header

ENUM

ENUM Suffix

Add

Priority / Weight

LDAP Search Attribute

LDAP Search Regex Pattern

LDAP Search Regex Result

SIP Server Profile

Next Hop Address

Transport

1

VoIPSP

10.64.102.241:

None

Delete

Finish

7.6. Administer Media Rules

Media Rules define RTP media packet parameters such as codec prioritization and packet encryption techniques. These rules will be applied to the End Point Policy Groups configured in **Section 7.7**.

Navigate to **Domain Policies** → **Media Rules** in the left pane. In the center pane, select the rule **avaya-low-med-enc** and click the **Clone** button. Input an appropriate name, e.g., **SRTP**. Click **Finish**. The **Encryption** tab for the SRTP media rule is configured as seen below.

Device: SBCE812 ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
 Application Rules
 Border Rules
 Media Rules
 Security Rules
 Signaling Rules
 Charging Rules
 End Point Policy Groups
 Session Policies
▸ TLS Management
▸ Network & Flows
▸ DMZ Services
▸ Monitoring & Logging

Media Rules: SRTP

Add

Rename Clone Delete

Media Rules

default-low-med
default-low-med-...
default-high
default-high-enc
avaya-low-med-...
SRTP

Click here to add a description.

Encryption Codec Prioritization Advanced QoS

Audio Encryption

Preferred Formats SRTP_AES_CM_128_HMAC_SHA1_80

Encrypted RTCP ☒

MKI ☐

Lifetime Any

Interworking ☒

Symmetric Context Reset ☒

Key Change in New Offer ☐

Video Encryption

Preferred Formats SRTP_AES_CM_128_HMAC_SHA1_80

Encrypted RTCP ☐

MKI ☐

Lifetime Any

Interworking ☒

Symmetric Context Reset ☒

Key Change in New Offer ☐

Miscellaneous

Capability Negotiation ☐

Edit

RH: Reviewed
SPOC 11/22/2021

Solution & Interoperability Test Lab Application Notes
©2021 Avaya Inc. All Rights Reserved.

45 of 90
MD500LiRWCMSM81

7.7. Administer End Point Policy Groups

End Point Policy Groups associate the different sets of rules (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE. For these application notes, a media rule will be configured to the policy group which is applied in **Section 7.10 End Point Flows**.

To create a new group, navigate to **Domain Policies**→ **End Point Policy Groups** in the left pane. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new group, e.g., **SRTP**, followed by the **Policy Group** window. Select **SRTP**, the media rule from **Section 7.6 for Media Rule**. Click **Finish**.

The new endpoint policy group, named **SRTP**, is shown below and is assigned the **SRTP** media rule configured in **Section 7.6**.

The screenshot shows the Avaya SBCE management interface. The left sidebar contains a navigation menu with 'Domain Policies' expanded, showing 'End Point Policy Groups' in red. The main area displays the 'Edit Policy Set' dialog box. The dialog box has the following fields:

- Application Rule: default
- Border Rule: default
- Media Rule: SRTP
- Security Rule: default-low
- Signaling Rule: default
- Charging Rule: None
- RTCP Monitoring Report Generation: Off

A 'Finish' button is located at the bottom of the dialog box. In the background, a table lists policy groups. The 'SRTP' group is highlighted in red.

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	default	default	SRTP	default-low	default	None	Off	Edit

7.8. Administer Media Interfaces

Media interfaces are created to specify IP addresses and port range which SBCE will accept media streams. Separate media interfaces are needed for public and private interfaces. Navigate to **Networks & Flows → Media Interface** to define a new Media Interface. During the Compliance Testing the following interfaces were defined.

- **InternalSIPTrunk:** Interface used by Session Manager to send and receive media.
- **InternalSIPUsers-RW:** Interface used by Session Manager to send and receive media for remote workers.
- **ExternalSIPTrunk:** Interface used by the VoIPSP to send and receive media
- **ExternalSIPUsers-RW:** External interface used by remote workers.

Device: SBCE812 ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
▸ Network & Flows
 Network Management
 Media Interface
 Signaling Interface
 End Point Flows
 Session Flows
 Advanced Options
▸ DMZ Services
▸ Monitoring & Logging

Media Interface

Media Interface

Add

Name	Media IP Network	Port Range	Edit	Delete
InternalSIPTrunk	10.64.110.242 Internal (A1, VLAN 0)	35000 - 40000	Edit	Delete
InternalSIPUsers-RW	10.64.110.243 Internal (A1, VLAN 0)	35000 - 40000	Edit	Delete
ExternalSIPUsers-RW	10.64.102.243 External-B1 (B1, VLAN 0)	35000 - 40000	Edit	Delete
ExternalSIPTrunk	10.64.102.242 External-B1 (B1, VLAN 0)	35000 - 40000	Edit	Delete

7.9. Administer Signaling Interfaces

A signaling interface defines an IP address, protocols and listen ports that the SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the SBCE. Navigate to **Networks & Flows** → **Signaling Interface** to define a new **Signaling Interface**. During the Compliance Testing the following interfaces were defined. The signaling interfaces used for this solution are listed below.

- **InternalSIPTrunk**: Interface used by Session Manager to send and receive signaling.
- **InternalSIPUsers-RW**: Interface used by Session Manager to send and receive signaling to remote workers.
- **ExternalSIPTrunk**: Interface used by the service provider e.g., **VoIPSP** to send and receive signaling.
- **ExternalSIPUsers-RW**: Interface used by remote workers to send and receive signaling.

Device: SBCE812 ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
▸ Network & Flows
 Network Management
 Media Interface
 Signaling Interface
 End Point Flows
 Session Flows
 Advanced Options
▸ DMZ Services
▸ Monitoring & Logging

Signaling Interface

Signaling Interface

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
ExternalSIPTrunk	10.64.102.242 External-B1 (B1, VLAN 0)	5060	5060	---	None	Edit Delete
InternalSIPTrunk	10.64.110.242 Internal (A1, VLAN 0)	5060	5060	5061	InternalServer	Edit Delete
InternalSIPUsers-RW	10.64.110.243 Internal (A1, VLAN 0)	5060	5060	5061	InternalServer	Edit Delete
ExternalSIPUser-RW	10.64.102.243 External-B1 (B1, VLAN 0)	5060	5060	5061	ExternalServer	Edit Delete

7.10. Administer End Point Flows

End Point Flows determine the path to be followed by the packets traversing through the Avaya SBCE. These flows combine the different sets of rules and profiles previously configured, to be applied to the SIP traffic traveling in each direction.

In the navigation pane, click **Network & Flows** → **End Point Flows**. Select **Subscriber Flows** or **End Point Flows** depending on the type of flow created. Click **Add**.

7.10.1. Remote Worker Subscriber Flow

Subscriber End Point Flows refer to the actual endpoint devices, from which SIP messages originate and to which they are destined. End point devices may include hard phones, soft phone clients, and wireless handsets.

Create the SIP Users Remote Worker subscriber flow with the following inputs:

- **Flow Name:** Input an appropriate name e.g., **SIPUsers-RW**
- **Signaling Interface:** Select the external Remote Worker interface from **Section 7.9** e.g., **ExternalSIPUsers-RW**
- **Media Interface:** Select the external Remote Worker media interface from **Section 7.8** e.g., **ExternalSIPUsers-RW**
- **End Point Policy Group:** Select the external policy group (Incorporating the media rule) from **Section 7.6** e.g., **SRTP**
- **Routing Profile:** Select the Routing Profile from **Section 7.5.1** for Session Manager e.g., **Session Manager**
- **TLS Client Profile:** Select the client profile from **Section 7.3.1** e.g., **ExternalClient**

Click **Finish**.

Add Flow X

Criteria

Flow Name

SIPUsers-RW

URI Group

* ▼

User Agent

* ▼

Source Subnet

Ex: 192.168.0.1/24

*

Via Host

Ex: domain.com, 192.168.0.1/24

*

Contact Host

Ex: domain.com, 192.168.0.1/24

*

Signaling Interface

ExternalSIPUsers-RW ▼

Next

Add Flow

X

Profile

Source

☒ Subscriber
☐ Click To Call

Methods Allowed Before REGISTER

INFO

MESSAGE

NOTIFY

OPTIONS

Media Interface

ExternalSIPUsers-RW

Secondary Media Interface

None

Received Interface

None

End Point Policy Group

SRTP

Routing Profile

SessionManager

Optional Settings

TLS Client Profile

ExternalClient

Signaling Manipulation Script

None

Presence Server Address

Ex: domain.com, 192.168.0.101

Back

Finish

7.10.2. Session Manager Server Flows

Server End Point Flows refer to the IP call servers that connect to SIP trunk services.

Create the Session Manager server flow to Remote Workers with the following inputs:

- **Flow Name:** Input an appropriate name e.g., **SIPUsers-Session Manager**
- **SIP Server Profile:** Select the Server Profile for Session Manager from **Section 7.4.1** e.g., **SessionManager**
- **Received Interface:** Select the external Remote Worker signaling interface from **Section 7.9** e.g., **ExternalSIPUsers-RW**
- **Signaling Interface:** Select the internal Remote Worker signaling interface from **Section 7.9** e.g., **InternalSIPUsers-RW**
- **Media Interface:** Select the internal Remote Worker signaling interface from **Section 7.8** e.g., **InternalSIPUsers-RW**
- **End Point Policy Group:** Select the end point policy group (Incorporating the media rule) from **Section 7.7** e.g., **SRTP**
- **Routing Profile:** Select the **default** Routing Profile

Click **Finish**.

Add Flow

X

Flow Name	SIPUserstoSessionManager
SIP Server Profile	SessionManager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	ExternalSIPUsers-RW
Signaling Interface	InternalSIPUsers-RW
Media Interface	InternalSIPUsers-RW
Secondary Media Interface	None
End Point Policy Group	SRTP
Routing Profile	default
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

Finish

7.10.3. VoIPSP Server Flows

For illustrative purposes, the VoIPSP flows were created as such:

View Flow: VoIPSP-SessionManager X

Criteria

Flow Name	VoIPSP-SessionManager
Server Configuration	SessionManager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	ExternalSIPTrunk

Profile

Signaling Interface	InternalSIPTrunk
Media Interface	InternalSIPTrunk
Secondary Media Interface	None
End Point Policy Group	S RTP
Routing Profile	VoIPSP
Topology Hiding Profile	To SMGR
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input checked="" type="checkbox"/>

View Flow: SessionManager-VoIPSP X

Criteria

Flow Name	SessionManager-VoIPSP
Server Configuration	VoIPSP
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	InternalSIPTrunk

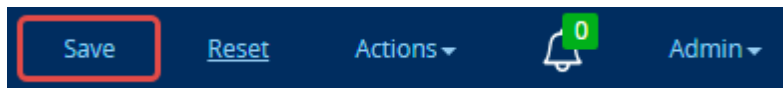
Profile

Signaling Interface	ExternalSIPTrunk
Media Interface	ExternalSIPTrunk
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	SessionManager
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

8. Configure AudioCodes Mediant 500Li Analog Gateway

This section describes Mediant 500Li configuration for the test environment.

Note: It is **recommended** to save any configuration changes to flash memory after they have been applied by pressing the **SAVE** button in the top left of corner of the management console. If the configuration has been changed, the **SAVE** button is outlined in red. Click the **SAVE** button to burn the new configuration to flash memory. If the configuration change requires a reset, the **RESET** button next to the **SAVE** button will be outlined in red and should be initiated.



8.1. Initial Network Setup

Initial network administration is done via the command line interface. See **document [4]** in **Section 11 Additional References** for further information.

The scope of Mediant 500Li Interoperability tests only includes analog line functionality. As such, the Interoperability test initial configuration includes only that needed for analog functionality and is documented here.

8.1.1. Assumptions

Mediant 500Li is located outside of the enterprise in the remote worker configuration. If the device is connected to the open internet, it is **highly** recommended to modify the access-list to follow your network security guidelines. Consult references **[5]** and **[6]** for access-list configuration information.

8.1.2. Changes to the configuration example below

Change the following parameters to reflect the numbering scheme of your network:

- **a.a.a.a** = IP address of Mediant 500Li
- **b.b.b.b** = subnet mask (ex. 255.255.255.0)
- **c.c.c.c** = primary DNS address
- **d.d.d.d** = secondary DNS address
- **e.e.e.e** = default gateway

8.1.3. CLI Configuration

Follow the process to initially configure Mediant 500Li IP address. CLI commands below change the factory default network settings. Once complete, the web interface can be accessible through the network.

- Set the ethernet port on your laptop to DHCP
- Connect an ethernet cable from your laptop into the first yellow port on Mediant 500Li. It should be labeled Sx/GE LAN 1. Mediant 500Li is set to provide a DHCP address in the range of 192.168.0.3 – 192.168.0.8.
- SSH into the MSBR via the following commands:

```
ssh Admin@192.168.0.1  
Password: as appropriate
```

```
M500Li> en  
Password: as appropriate
```

- Enter the following commands:

```
configure data
access-list voip permit ip any any
interface gigabitethernet 0/0
ip address a.a.a.a b.b.b.b
ip name-server c.c.c.c d.d.d.d
ip access-group voip in
exit
ip route 0.0.0.0 0.0.0.0 e.e.e.e gigabitethernet 0/0 10
exit
```

- Verify you can log into the GUI via the IP address assigned to **gigabitethernet 0/0**
- Open a new terminal session and ssh into the CLI via the IP address assigned to **gigabitethernet 0/0**

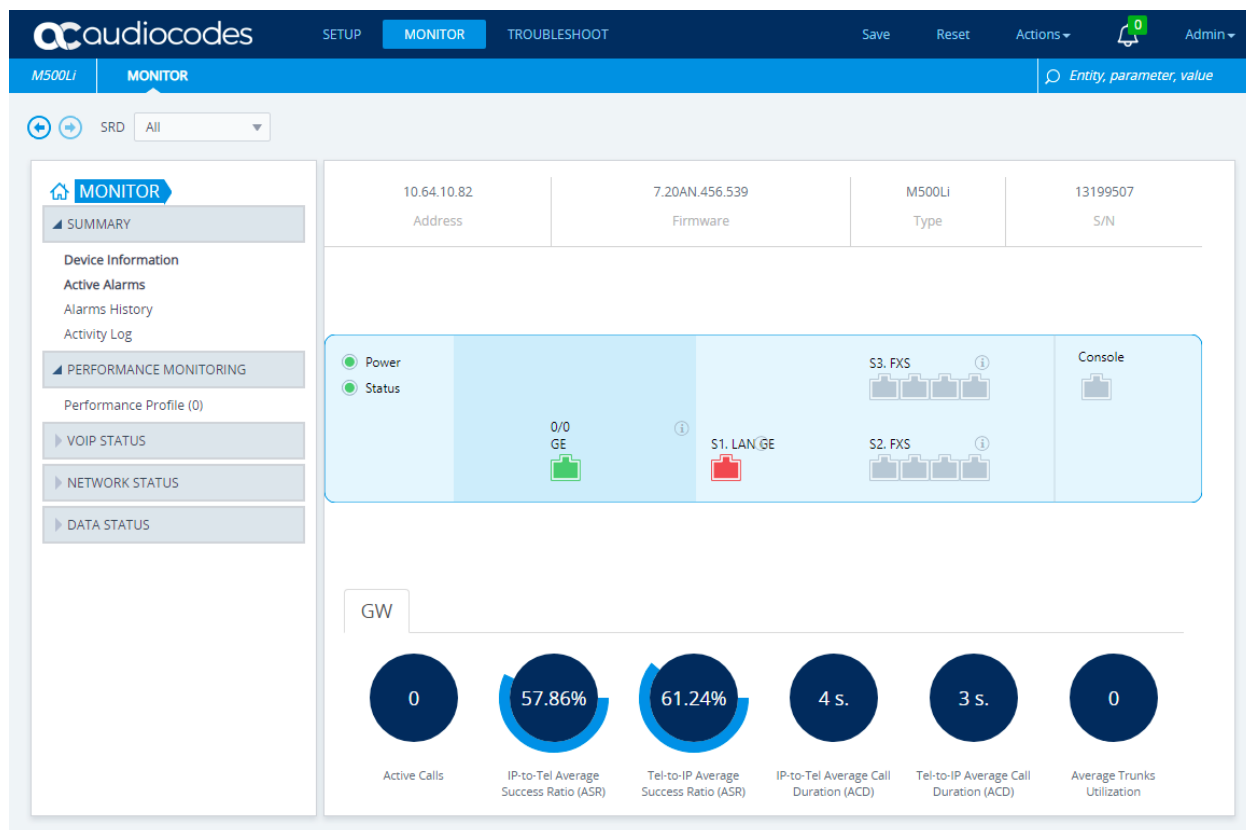
```
configure data
interface GigabitEthernet 1/1
shutdown
exit
exit
write
```

NOTE: Shutting down the LAN port after IP configuration is optional

NOTE: The **write** command writes the current configuration to flash.

8.2. Verify/Upgrade Firmware Version

Configuration of the AudioCodes Mediant 500Li is done via web administrative console. Type in `http://<IP-address>` in a web browser, where `<IP-address>` is the IP Address of AudioCodes Mediant 500Li. Enter **Admin** as the username and the appropriate password. Click **Log In**. Once logged in, click on the **MONITOR** button in the title bar. The firmware version is displayed.



The firmware version used in Interoperability testing is **7.20AN.456.539**. To upgrade Mediant 500Li software, consult **document [4]** in **Section 11 Additional References** for instructions.

8.3. Set System Time and Date

Click on the **SETUP** button in the title bar. Select **ADMINISTRATION** in the toolbar. The time and date panel displays.

- Select **Enable** for **Enable NTP**
- Select an appropriate **Primary NTP Server Address**
- Select the appropriate **UTC Offset** and **DST Mode**
- Select **Day of month** for the **DST mode**
- Input the appropriate **Day of Month Start** and **Day of Month End**

Click **APPLY**. The local time should display correctly

The screenshot shows the Audiocodes M500Li Administration interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The 'ADMINISTRATION' tab is selected. The left sidebar shows a tree view with 'TIME & DATE' expanded. The main content area displays the 'TIME & DATE' configuration page. The 'LOCAL TIME' section shows the current local time as 2021-06-08 13:41:36. The 'TIME ZONE' section shows the UTC time as 8 Jun, 2021 19:41:36. The 'NTP SERVER' section includes the 'Enable NTP' dropdown (set to 'Enable'), the 'Primary NTP Server Address (IP or FQDN)' text field (containing 'pool.ntp.org'), and the 'Secondary NTP Server Address (IP or FQDN)' text field. The 'DATE HEADER TIME SYNC' section includes the 'Synchronize Time from SIP Date Header' dropdown (set to 'Disable') and the 'Time Synchronization Interval [sec]' text field (containing '900'). Red boxes highlight the 'Enable NTP' dropdown, the 'Primary NTP Server Address' text field, the 'UTC Offset' and 'Daylight Saving Time' settings, and the 'Day of Month Start' and 'Day of Month End' date pickers.

8.4. Administer Syslog Settings

Click on **TROUBLESHOOT** in the title bar. Select **LOGGING** → **Logging Settings** in the left pane.

- 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., **AudioCodes Syslog Viewer**
 - Set **VoIP Debug Level** to **Detailed**
 - Under the **ACTIVITY TYPES TO REPORT** subsection, check **Select All**
- Click **APPLY**.

The screenshot shows the AudioCodes M500LI Troubleshoot interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT' (highlighted in blue). A 'Save' button is visible in the top right. The left sidebar shows a 'MESSAGE LOG' section with 'LOGGING' selected, and 'Logging Settings' is the active sub-tab. The main content area is titled 'Logging Settings' and contains several sections: 'SYSLOG' with fields for 'Enable Syslog' (set to 'Enable'), 'Syslog Server IP' (set to '10.64.110.47'), 'Syslog Server Port' (514), 'Log Severity Level' (Notice), 'Syslog CPU Protection' (Enabled), 'Syslog Optimization' (Disabled), 'VoIP Debug Level' (set to 'Detailed'), and 'Debug Level High Threshold' (90); 'ACTIVITY TYPES TO REPORT' with 'Select All' checked and several other options checked; 'DEBUG RECORDING' with fields for 'Debug Recording Destination IP' (0.0.0.0), 'Debug Recording Destination Port' (925), and 'Debug Recording Interface Name'; and 'CALL FLOW' with 'Call Flow Report Mode' set to 'Disable'. At the bottom right of the main content area are 'Cancel' and 'APPLY' buttons.

8.5. Administer Security

8.5.1. TLS Contexts

Click on **SETUP** in the title bar. Select **IP NETWORK** in the toolbar. Select **SECURITY** → **TLS Contexts** in the left pane. The default context displays.

- Click the **Edit** button (not shown)
 - Select **default** for the **NAME**
 - Select **TLSv1.0 TLSv1.1 TLSv1.2 and TLSv1.3** for the **TLS Version**
- Click **APPLY**.

The screenshot shows the Audiocodes M500Li configuration interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The left sidebar shows 'IP NETWORK', 'SIGNALING & MEDIA', and 'ADMINISTRATION'. The 'SECURITY' section is expanded, showing 'TLS Contexts [default]'. The 'GENERAL' tab is selected, displaying fields for 'Index' (0), 'Name' (default), 'TLS Version' (TLSv1.0 TLSv1.1 TLSv1.2 and TLSv1.3), 'DTLS Version' (Any), 'Cipher Server' (DEFAULT), 'Cipher Client' (DEFAULT), 'Cipher Server TLS1.3' (TLS_AES_256_GCM_SHA384:TLS_C), 'Cipher Client TLS1.3' (TLS_AES_256_GCM_SHA384:TLS_C), 'Key Exchange Groups' (X25519:P-256:P-384:X448), 'Strict Certificate Extension Validation' (Disable), 'DH key Size' (2048), and 'TLS Renegotiation' (Enable). The 'OCSP' tab is also visible on the right, showing fields for 'OCSP Server' (Disable), 'Primary OCSP Server' (0.0.0.0), 'Secondary OCSP Server' (0.0.0.0), 'OCSP Port' (2560), and 'OCSP Default Response' (Reject). At the bottom, there are links for 'Certificate Information >>', 'Change Certificate >>', and 'Trusted Root Certificates >>'.

Note: Links at the bottom of the page are used for certificate administration as detailed in **Section 8.6.1**.

[Certificate Information >>](#)

[Change Certificate >>](#)

[Trusted Root Certificates >>](#)

8.5.2. Administer Security Settings

Click on **SETUP** in the title bar. Select **IP NETWORK** in the toolbar. Select **SECURITY** → **Security Settings** in the left pane.

- Select **Enable** for **TLS Client Verify Server Certificate**
Click **APPLY**.

The screenshot shows the Audiocodes MD500Li web interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The left sidebar shows 'IP NETWORK' selected, with 'SECURITY' and 'Security Settings' highlighted. The main content area is titled 'Security Settings' and contains two tabs: 'SIP OVER TLS' and 'TLS GENERAL'. Under 'SIP OVER TLS', the 'TLS Client Verify Server Certificate' dropdown is set to 'Enable' and is highlighted with a red box. Other settings include 'TLS Client Re-Handshake Interval' (0), 'TLS Mutual Authentication' (Disable), 'Peer Host Name Verification Mode' (Disable), and 'TLS Remote Subject Name'. Under 'TLS GENERAL', 'Strict Certificate Extension Validation' is set to 'Disable', 'TLS Expiry Check Start (days)' is 60, and 'TLS Expiry Check Period (days)' is 7. A 'MANAGEMENT' section at the bottom has 'Enable Management Two Factor Authentication' set to 'Disable'. 'Save' and 'Reset' buttons are in the top right, and 'Cancel' and 'APPLY' buttons are at the bottom right.

Category	Setting	Value
SIP OVER TLS	TLS Client Re-Handshake Interval	0
	TLS Mutual Authentication	Disable
	Peer Host Name Verification Mode	Disable
	TLS Client Verify Server Certificate	Enable
	TLS Remote Subject Name	
TLS GENERAL	Strict Certificate Extension Validation	Disable
	TLS Expiry Check Start (days)	60
	TLS Expiry Check Period (days)	7
MANAGEMENT	Enable Management Two Factor Authentication	Disable

8.6. Administer Media

Media configuration administers SRTP connection parameters to the proxy server.

8.6.1. Administer Media Security

Select **SETUP** in the title bar. Select **SIGNALING & MEDIA** in the toolbar. Select **MEDIA** → **Media Security** in the left pane.

- Select **Enable** for **Media Security**
- Select **Mandatory** for **Media Security Behavior**.
- Select **Inactive** for **Encryption on Transmitted RTCP Packets**

Click **APPLY**.

The screenshot displays the Audiocodes configuration interface for Media Security. The top navigation bar includes tabs for SETUP, MONITOR, TROUBLESHOOT, and a Save button. The left sidebar shows a tree view with categories like TOPOLOGY VIEW, CORE ENTITIES, CODERS & PROFILES, GATEWAY, SIP DEFINITIONS, MESSAGE MANIPULATION, MEDIA, and INTRUSION DETECTION. The MEDIA section is expanded, showing sub-items like RTP/RTCP Settings, Voice Settings, Fax/Modem/CID Settings, Media Settings, DSP Settings, Quality of Experience, and INTRUSION DETECTION. The main content area is titled 'Media Security' and contains several sections: GENERAL, AUTHENTICATION & ENCRYPTION, MASTER KEY IDENTIFIER, and GATEWAY SETTINGS. In the GENERAL section, 'Media Security' is set to 'Enable' and 'Media Security Behavior' is set to 'Mandatory'. In the AUTHENTICATION & ENCRYPTION section, 'Encryption on Transmitted RTCP Packets' is set to 'Inactive'. The MASTER KEY IDENTIFIER section shows 'Master Key Identifier (MKI) Size' as 0 and 'Symmetric MKI' as Disable. The GATEWAY SETTINGS section shows 'Enable Rekey After 181' as Disable. The 'APPLY' button is located at the bottom right of the configuration area.

8.6.2. Install Certificates

Note: The certificate configuration tested used one-way authentication.

Note: The Certificate Authority used for Interoperability tests is Avaya Session Manager. Session Manager CA certificate file generation is not covered here. Consult reference [2] in **Section 11**. Please note that without this certificate, TLS/SRTP will not work.

Click on **SETUP** in the title bar. Select **IP NETWORK** in the toolbar. Select **SECURITY** → **TLS Contexts** pane, and select **Trusted Root Certificates** in the bottom of the pane (not shown).

Click the **Import** button and select the CA certificate file.

The screenshot shows the Avaya Session Manager GUI. The top navigation bar includes 'audiocodes', 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The 'SETUP' button is highlighted with a red box. Below the navigation bar, the 'IP NETWORK' tab is selected. The left sidebar shows a tree view with 'CORE ENTITIES', 'SECURITY', 'QUALITY', 'DNS', 'WEB SERVICES', 'RADIUS & LDAP', and 'ADVANCED'. The 'SECURITY' section is expanded, showing 'TLS Contexts (1)'. The main content area displays the 'Trusted Root Certificates' list for 'TLS Context [#0]'. The list has columns for INDEX, SUBJECT, ISSUER, and EXPIRES. The 'Import' button is highlighted with a red box. Below the list, there is a 'Selected Row #0' section.

INDEX	SUBJECT	ISSUER	EXPIRES
0	CA_7B	RootCA	1/01/2030
1	RootCA	RootCA	1/01/2030
2	AddTrust External CA Root	AddTrust External CA Root	5/30/2020
3	DigiCert Global Root CA	DigiCert Global Root CA	11/10/2031
4	DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038
5	DigiCert SHA2 High Assurance Se	DigiCert High Assurance EV Root	10/22/2028
6	GeoTrust Global CA	GeoTrust Global CA	5/21/2022

The imported certificate should display in the Trusted Root Certificates list.

SETUP

MONITOR

TROUBLESHOOT

Save

Reset

Actions

0

Admin

MS00Li

IP NETWORK

SIGNALING & MEDIA

ADMINISTRATION

Entity, parameter, value

SRD

All

NETWORK VIEW

CORE ENTITIES

NAT Translation (0)

SECURITY

TLS Contexts (1)

Security Settings

QUALITY

DNS

WEB SERVICES

RADIUS & LDAP

ADVANCED

TLS Context [#0] > Trusted Root Certificates

View

Import

Export

Remove

INDEX	SUBJECT	ISSUER	EXPIRES
10	thawte Primary Root CA	thawte Primary Root CA	7/16/2036
11	VeriSign, Inc.	VeriSign, Inc.	8/01/2028
12	VeriSign Class 3 Public Primary	VeriSign Class 3 Public Primary	7/16/2036
13	System Manager CA	System Manager CA	7/15/2029

Page 2 of 2

10

View 11 - 14 of 14

Selected Row #13

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

5c:fb:ae:03:6c:9e:8f:5f

RH: Reviewed
SPOC 11/22/2021

Solution & Interoperability Test Lab Application Notes
©2021 Avaya Inc. All Rights Reserved.

64 of 90
MD500LiRWCMSM81

8.6.3. Administer Media Settings

Click on **SETUP** in the title bar. Select **Signaling & Media** in the toolbar. Select **MEDIA** → **Media Settings** in the left pane.

- Select **Enable** for **Enable Early Media**
Click **APPLY**.

The screenshot displays the Audiocodes M500Li configuration interface. The top navigation bar includes tabs for SETUP, MONITOR, and TROUBLESHOOT, with a 'Save' button highlighted. Below this, a secondary bar shows 'IP NETWORK', 'SIGNALING & MEDIA', and 'ADMINISTRATION'. The left sidebar contains a 'TOPOLOGY VIEW' section with various settings categories, including 'MEDIA', which is expanded to show 'Media Security', 'RTP/RTCP Settings', 'Voice Settings', 'Fax/Modem/CID Settings', 'Media Settings' (highlighted), 'DSP Settings', 'Quality of Experience', and 'INTRUSION DETECTION'. The main content area is titled 'Media Settings' and is divided into three sections: GENERAL, GATEWAY SETTINGS, and ROBUSTNESS. In the GATEWAY SETTINGS section, the 'Enable Early Media' option is set to 'Enable' and is highlighted with a red box. Other settings include 'NAT Traversal' (Disable NAT), 'Enable Continuity Tones' (Disable), 'Number of Media Channels' (-1), 'Enforce Media Order' (Disable), 'SDP Session Owner' (AudiocodesGW), 'Multiple Packetization Time Format' (None), 'Inbound Media Latch Mode' (Dynamic), 'New RTP Stream Packets' (3), 'New RTCP Stream Packets' (3), 'New SRTP Stream Packets' (3), 'New SRTCP Stream Packets' (3), 'Timeout To Relatch RTP (msec)' (200), 'Timeout To Relatch SRTP (msec)' (200), 'Timeout To Relatch Silence (msec)' (10000), and 'Timeout To Relatch RTCP (msec)' (10000). At the bottom of the main content area, there are 'Cancel' and 'APPLY' buttons.

8.7. Administer SIP Definitions

8.7.1. General settings

Click **SETUP** in the title bar. Select **Signaling & Media** in the toolbar. Select **SIP DEFINITIONS → SIP Definitions General Settings** in the left pane.

- Select **Ignore** for **Broken Connection Mode**. Interoperability Testing used **Disconnect** which will cause Mediant 500Li to disconnect the call if RTP is not detected within the time specified in the Broken Connection Timeout. **Note:** The Default Broken Connection Timeout is 10 seconds (100 x 100ms). This does not affect the results of the interoperability testing.

Click **APPLY**.

The screenshot shows the Audiocodes M500Li web interface for configuring SIP Definitions. The top navigation bar includes 'SETUP', 'MONITOR', 'TROUBLESHOOT', 'Save', 'Reset', 'Actions', and 'Admin'. The left sidebar shows the 'SIP DEFINITIONS' menu with 'SIP Definitions General Settings' selected. The main content area is titled 'SIP Definitions General Settings' and contains several sections:

- GENERAL**: Send Reject (503) upon Overload (Enable), Retry-After Time (0), Fake Retry After (0), Remote Management by SIP NOTIFY (Disable).
- GATEWAY SESSION EXPIRES**: Session-Expires Time (0), Minimum Session-Expires (90), Session Expires Method (re-INVITE), Session Expires Disconnect Time (32).
- GATEWAY SETTINGS**: PRACK Mode (Supported), Early 183 (Disable), 183 Message Behavior (Progress), 3xx Behavior (Forward), Call Transfer using re-INVITEs (Disable), First Call Ringback Tone ID (-1).
- DISCONNECT SUPERVISION**: Broken Connection Mode (Disconnect), Broken Connection Timeout [100 msec] (100).
- MICROSOFT PRESENCE**: Presence Publish IP Group ID (-1), Microsoft Presence Status (Disable).

At the bottom of the main panel are 'Cancel' and 'APPLY' buttons.

8.7.2. Transport Settings

Click on **SETUP** in the title bar. Select **Signaling & Media** in the toolbar. Select **SIP DEFINITIONS** → **Transport Settings** in the left pane.

- Select **Enable** for **SIPS**
- Select **TLS** for **SIP Transport Type**
- Select **5061** for the **SIP Destination Port**

Click **APPLY**.

The screenshot shows the Audiocodes MS500Li web interface. The top navigation bar includes tabs for SETUP, MONITOR, TROUBLESHOOT, and a Save button. The left sidebar shows the navigation menu with 'SIP DEFINITIONS' expanded and 'Transport Settings' selected. The main configuration area is titled 'Transport Settings' and contains three tabs: GENERAL, TCP CONNECTION, and RETRANSMISSION. The GENERAL tab is active, showing settings for SIP NAT Detection, SIPS, SIP Transport Type, ENUM Resolution, SIP 408 Response upon non-INVITE, DNS Query Type, and SIP Destination Port. The SIPS, SIP Transport Type, and SIP Destination Port settings are highlighted with red boxes. The TCP CONNECTION tab shows settings for TCP/TLS Connection Reuse, TCP Timeout, Reliable Connection Persistent Mode, and Fake TCP alias. The RETRANSMISSION tab shows settings for SIP T1 Retransmission Timer, SIP T2 Retransmission Timer, and SIP Maximum RTX.

Setting	Value
SIP NAT Detection	Enable
SIPS	Enable
SIP Transport Type	TLS
ENUM Resolution	e164.arpa
SIP 408 Response upon non-INVITE	Enable
DNS Query Type	A-Record
SIP Destination Port	5061
TCP/TLS Connection Reuse	Enable
TCP Timeout	0
Reliable Connection Persistent Mode	Disable
Fake TCP alias	Disable
SIP T1 Retransmission Timer [msec]	500
SIP T2 Retransmission Timer [msec]	4000
SIP Maximum RTX	7

8.7.3. Proxy Registration

Click on **SETUP** in the title bar. Select **Signaling & Media** in the toolbar. Select **SIP DEFINITIONS → Proxy & Registration** in the left pane.

- Select **Enable** for **Enable Registration**

Click **Apply**.

The screenshot displays the Audiocodes configuration interface for SIP settings. The top navigation bar includes 'audiocodes', 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. Below this, a secondary bar shows 'MS00LI', 'IP NETWORK', 'SIGNALING & MEDIA' (selected), and 'ADMINISTRATION'. A search bar on the right contains the text 'Entity, parameter, value'. The left sidebar, titled 'TOPOLOGY VIEW', lists various configuration categories, with 'Proxy & Registration' highlighted under 'SIP DEFINITIONS'. The main content area, titled 'Proxy & Registration', is divided into several sections: 'GENERAL' (containing settings like Redundancy Mode, Proxy IP List Refresh Time, Proxy DNS Query Type, Number of RTX Before Hot-Swap, Use Proxy IP as Host, User-Information Usage, Add Empty Authorization Header, Gateway Name, Use Gateway Name for OPTIONS, and Challenge Caching Mode), 'GATEWAY PROXY' (containing settings like Use Default Proxy, Proxy Name, Prefer Routing Table, Use Routing Table for Host Names and Profiles, Always Use Proxy, and Enable Fallback to Routing Table), 'AUTHENTICATION' (containing User Name, Password, and Cnonce fields), 'GATEWAY AUTHENTICATION' (containing Authentication Mode), and 'GATEWAY REGISTRATION' (containing Enable Registration and Registrar Name). The 'Enable Registration' dropdown in the 'GATEWAY REGISTRATION' section is highlighted with a red box and set to 'Enable'. At the bottom of the main content area, there are 'Cancel' and 'APPLY' buttons.

8.7.4. Administer Call Detail Records

Call Detail Records (CDR) contains vital statistic information on calls made from the device. Configure call detail records for any needed troubleshooting. Enable the Syslog feature as in **Section 8.4** and configure a collecting server address. Refer to **Reference [4]** in **Section 11** for details.

Click on **TROUBLESHOOT** in the title bar. Select **CALL DETAIL RECORD** → **Call Detail Record Settings** in the left pane.

- Select **Start & End & Connect** for the **CDR Report Level**

Click **APPLY**.

The screenshot shows the Audiocodes M500Li Troubleshoot interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT' (highlighted). The 'TROUBLESHOOT' section has a 'Save' button highlighted with a red box. The left sidebar shows the 'CALL DETAIL RECORD' section with 'Call Detail Record Settings' selected. The main content area is titled 'Call Detail Record Settings' and contains several configuration sections:

- CDR GENERAL SETTINGS:** Includes fields for 'Call-End CDR SIP Reasons Filter', 'Call-End CDR Zero Duration Filter' (set to 'Disable'), 'Call Success SIP Reasons', 'Call Failure SIP Reasons', 'Call Success Internal Reasons', 'Call Failure Internal Reasons', 'No User Response Before Connect' (set to 'Call Success'), 'No User Response After Connect' (set to 'Call Failure'), 'Call Transferred Before Connect' (set to 'Call Failure'), and 'Call Transferred After Connect' (set to 'Call Success').
- RADIUS ACCOUNTING SETTING:** Includes 'Enable RADIUS Access Control' (set to 'Disable'), 'RADIUS Accounting Type' (set to 'At Call Release'), and 'AAA Indications' (set to 'None').
- REST CDR REPORT:** Includes 'REST CDR Report Level' (set to 'None') and 'REST CDR HTTP Server Name'.
- CDR LOCAL STORAGE:** Includes 'File Size (KBytes)' (set to '1024'), 'Number Of Files' (set to '5'), and 'Rotation period (min)' (set to '60').
- SYSLOG CDR REPORTS:** Includes 'CDR Syslog Server IP Address' (set to '::') and 'CDR Report Level' (set to 'Start & End & Connect', highlighted with a red box). The 'Media CDR Report Level' is set to 'None'.

At the bottom right of the settings area are 'Cancel' and 'APPLY' buttons.

8.8. Administer Coders Groups

The default Coders Group can have all needed coders assigned and used. Interoperability testing used multiple Coders Groups with different coders to assign to the Tel Profile administered in **Section 8.8.1**.

Select **SETUP** from the title bar. Select **Signaling & Media** from the toolbar. Select **CODERS & PROFILES → Coders Groups**.

- Select the desired coder group in the **Coder Group Name**. The default Coders Group is **0:AudioCodersGroups_0**
- Select the **Coder Name** in the dropdown for each row. For the default Coders Group, **G.711U-law**, **G.729**, and **G.711A-law**.

Click **APPLY**.

audiocodes SETUP MONITOR TROUBLESHOOT Save Reset Actions 0 Admin

M500Li IP NETWORK SIGNALING & MEDIA ADMINISTRATION Entity, parameter, value

SRD All

TOPOLOGY VIEW

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

Coders Groups

Coder Group Name: 0 : AudioCodersGroups_0 Delete Group

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	Coder Specific
G.711U-law	20	64	0	Disabled	
G.729	20	8	18	Disabled	
G.711A-law	20	64	8	Disabled	

Cancel APPLY

8.8.1. Administer Tel Profiles

Tel profiles are used to assign different Coder Groups and specify Fax signalling method.

NOTE: The Tel Profile is not needed if using the default Coder Group only.

Select **SETUP** from the title bar. Select **Signaling & Media** from the toolbar. Select **CODERS & PROFILES** → **Tel Profiles**

- Click the + **NEW** button (not shown)
- Select an appropriate **Name** e.g., **TelProfile_1**
- Select the desired **Coders Group**
- Select **G.711 Transport** for **Fax Signaling Method**

Click **APPLY**.

The screenshot displays the Audiocodes M500LI web interface. At the top, there is a navigation bar with tabs: SETUP, MONITOR, and TROUBLESHOOT. Below this is a toolbar with buttons: Save, Reset, Actions, and Admin. The main content area is titled 'Tel Profiles [TelProfile_1]'. It contains several sections: GENERAL, SIGNALING, BEHAVIOR, IP SETTINGS, ECHO CANCELER, and JITTER BUFFER. The GENERAL section includes fields for Index (1), Name (TelProfile_1), Profile Preference (1), Fax Signaling Method (G.711 Transport), Enable Digit Delivery (Disable), Dial Plan Index (-1), and Call Priority Mode (Disable). The IP SETTINGS section includes Coder Group (#0 [AudioCodersGroups_0]), RTP IP DiffServ (46), Signaling DiffServ (24), Enable Early Media (Enable), and Progress Indicator to IP (dropdown). The ECHO CANCELER section includes Echo Canceled (Line Echo Canceller) and EC NLP Mode (Adaptive NLP). The JITTER BUFFER section includes Dynamic Jitter Buffer Minimum Delay (ms) (10). The APPLY button is highlighted.

8.9. Configure Core Administration

Core administration will configure Media and signaling parameters

8.9.1. Media Realm

Click on **SETUP** in the title bar. Select **Signaling & Media** in the toolbar. Select **CORE ENTITIES → Media Realms** in the left pane. Click **Edit** (not shown)

- Input an appropriate **Name**
- Select the default **Ipv4 Interface Name**
- Input **6000** for the **UDP Port Range Start**
- Input **20** for **Number Of Media Session Legs**
- Select **Yes** for the **Default Media Realm**

Click **Apply**.

The screenshot shows the Audiocodes Management Console interface. The top navigation bar includes 'audiocodes', 'SETUP', 'MONITOR', 'TROUBLESHOOT', and buttons for 'Save', 'Reset', 'Actions', and 'Admin'. Below this is a secondary navigation bar with 'MS00LI', 'IP NETWORK', 'SIGNALING & MEDIA', and 'ADMINISTRATION'. A search bar on the right contains the text 'Entity, parameter, value'. The left sidebar shows a tree view with 'CORE' expanded, and 'Media Realms' selected. The main content area displays the 'Media Realms [DefaultRealm]' configuration page. It is divided into two tabs: 'GENERAL' and 'QUALITY OF EXPERIENCE'. The 'GENERAL' tab contains the following fields: 'Index' (0), 'Name' (DefaultRealm), 'Topology Location' (Down), 'IPv4 Interface Name' (#0 [main-vrf-ipv4]), 'IPv6 Interface Name' (--), 'UDP Port Range Start' (6000), 'Number Of Media Session Legs' (20), 'UDP Port Range End' (6199), 'TCP Port Range Start' (0), 'TCP Port Range End' (0), and 'Default Media Realm' (Yes). The 'QUALITY OF EXPERIENCE' tab contains 'QoE Profile' and 'Bandwidth Profile', both set to '--'. At the bottom of the 'GENERAL' tab, there are 'Cancel' and 'APPLY' buttons. A summary table at the bottom of the page shows the following values: 'UDP Port Range E...' (6199), 'TCP Port Range St...' (0), 'TCP Port Range End' (0), and 'Default Media Rea...' (Yes).

Parameter	Value
UDP Port Range E...	6199
TCP Port Range St...	0
TCP Port Range End	0
Default Media Rea...	Yes

8.9.2. SIP Interface

Click on **SETUP** in the title bar. Select **Signaling & Media** in the toolbar. Select **CORE ENTITIES** → **SIP Interfaces** in the left pane. Click **Edit** (not shown)

- Input an appropriate **Name**. Interoperability testing used **SIPInterface_0**
 - Select **#0 [DefaultRealm]** for the **Media Realm**
 - Select **#0 [main-vrf-ipv4]** for **Network Interface**
 - Input **0** for the **UDP Port** and **TCP Port** as interoperability testing used TLS
- Click **APPLY**.

The screenshot shows the Avaya M500Li interface with the 'SIP Interfaces [SIPInterface_0]' configuration window open. The window is divided into two main sections: 'GENERAL' and 'MEDIA'. The 'GENERAL' section contains fields for 'Index' (0), 'Name' (SIPInterface_0), 'Topology Location' (Down), 'Network Interface' (#0 [main-vrf-ipv4]), 'Application Type' (GW), 'UDP Port' (0), 'TCP Port' (0), 'TLS Port' (5061), 'Additional UDP Ports', and 'Additional UDP Ports Mode' (Always Open). The 'MEDIA' section contains 'Media Realm' (#0 [DefaultRealm]), 'Direct Media' (Disable), and 'SECURITY' settings including 'TLS Context Name' (#0 [default]), 'TLS Mutual Authentication', 'Message Policy' (--), 'User Security Mode' (Not Configured), 'Enable Un-Authenticated Registrations' (Not configured), and 'Max. Number of Registered Users' (-1). The 'Save' button in the top toolbar is highlighted with a red box. The 'APPLY' button at the bottom of the configuration window is also highlighted with a red box.

8.9.3. Proxy Set

Click on **SETUP** in the title bar. Select **Signaling & Media** in the toolbar. Select **CORE ENTITIES → Proxy Sets** in the left pane. Click **Edit** (not shown).

- Input an appropriate **Name**. Interoperability testing used **ProxySet_0**
- Select **#0 [SIPInterface_0]** for **Gateway Ipv4 SIP Interface**
- Select **#0 [default]** for **TLS Context Name**
- Select **Using OPTIONS** for **Proxy Keep-Alive**
- Input **120** for **Proxy Keep-Alive Time (sec)**

Click **APPLY**.

The screenshot shows the Audiocodes M500LI configuration interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The left sidebar shows the navigation tree with 'CORE ENTITIES' expanded, and 'Proxy Sets' selected. The main configuration area is titled 'Proxy Sets [ProxySet_0]'. It contains several sections: 'GENERAL' with fields for 'Index' (0), 'Name' (ProxySet_0), 'Gateway IPv4 SIP Interface' (#0 [SIPInterface_0]), 'Gateway IPv6 SIP Interface' (--), and 'TLS Context Name' (#0 [default]); 'REDUNDANCY' with fields for 'Redundancy Mode', 'Proxy Hot Swap' (Disable), 'Proxy Load Balancing Method' (Disable), and 'Min. Active Servers for Load Balancing' (1); 'KEEP ALIVE' with fields for 'Proxy Keep-Alive' (Using OPTIONS) and 'Proxy Keep-Alive Time [sec]' (120); and 'ADVANCED' with fields for 'Classification Input' (IP Address only), 'DNS Resolve Method', and 'Accept DHCP Proxy List' (Disable). The 'APPLY' button is highlighted at the bottom right of the configuration area.

In the **Proxy Sets** pane, select the **Proxy Address Items** link at the bottom of the pane. Click **Edit** (not shown):

- If the Mediant 500Li is located within the enterprise, input Session Manager IP address used in **Section 5.4** for **Proxy Address** e.g., **10.64.110.212** (not shown)
- If the Mediant 500Li is located in a remote location, input the SBCE external interface B1 IP address used by remote workers in **Section 7.2** for **Proxy Address** e.g., **10.64.102.243**
- Select **TLS** for the **Transport Type**
Click **APPLY**.

The screenshot displays the Audiocodes M500Li administration interface. The top navigation bar includes tabs for SETUP, MONITOR, and TROUBLESHOOT. The left sidebar shows a TOPOLOGY VIEW with various categories like CORE ENTITIES, SRDs, SIP Interfaces, Media Realms, Proxy Sets (1), and IP Groups (1). The main content area shows the 'Proxy Address' configuration window. The 'GENERAL' tab is active, displaying fields for Index (0), Proxy Address (10.64.102.243:5061), Transport Type (TLS), Proxy Priority (0), and Proxy Random Weight (0). The 'Proxy Address' and 'Transport Type' fields are highlighted with a red box. The 'Save' button in the top right is also highlighted with a red box. The bottom of the window has 'Cancel' and 'APPLY' buttons.

8.9.4. IP Groups

Click on **SETUP** in the title bar. Select **Signaling & Media** in the toolbar. Select **CORE ENTITIES → IP Groups** in the left pane. Click **Edit** (not shown)

- Input an appropriate **Name**. Interoperability testing used **Default_IPG**
- Select **#0 [ProxySet_0]** for **Proxy Set**
- Select **#0 [DefaultRealm]** for **Media Realm**
- Select **#0 [DefaultRealm]** for **Internal Media Realm**
- Input **avaya.com** for **SIP Group Name**
- Select **Enable** for **Proxy Keep-Alive using IP Group settings**

Click **APPLY**.

The screenshot shows the Avaya Aura Management GUI. The top toolbar includes buttons for 'SETUP', 'MONITOR', 'TROUBLESHOOT', 'Save', 'Reset', 'Actions', and 'Admin'. The left sidebar shows a navigation tree with 'CORE ENTITIES' expanded, leading to 'IP Groups'. The main window displays the 'IP Groups [Default_IPG]' configuration page. The 'GENERAL' tab is active, showing fields for 'Index' (0), 'Name' (Default_IPG), 'Topology Location' (Down), 'Proxy Set' (#0 [ProxySet_0]), 'IP Profile' (--), 'Media Realm' (#0 [DefaultRealm]), 'Internal Media Realm' (#0 [DefaultRealm]), 'Contact User', 'SIP Group Name' (avaya.com), and 'Created By Routing Server' (No). The 'QUALITY OF EXPERIENCE' tab is also visible, showing 'QoE Profile' (--), 'Bandwidth Profile' (--), and 'MESSAGE MANIPULATION' settings. The 'Proxy Keep-Alive using IP Group settings' is set to 'Enable'. A 'Save' button is highlighted in the top toolbar.

8.10. Administer Gateway

This section covers FXS port administration

8.10.1. Trunk Groups

Click on **SETUP** in the title bar. Select **Signaling & Media** in the toolbar. Select **Gateway → Trunks & Groups → Trunk Groups** in the left pane. Administer two analog extensions here.

Note: The module selection refers to specific FXS ports in the back of the Mediant 500Li hardware.

- Select **Module 2 FXS** for the **MODULE**
- Select **1** for the **CHANNELS**
- Input the extension from the SIP users administered in **Section 6.8.5** for the **PHONE NUMBER**
- Select **1** for the **TRUNK GROUP ID**
- Select **TelProfile_1** for the **TEL PROFILE NAME**
- Repeat input using the second user extension for **PHONE NUMBER** and **2** for **CHANNELS** to create the second extension

Click **APPLY**.

The screenshot shows the Audiocodes Mediant 500Li configuration interface. The top navigation bar includes 'audiocodes', 'SETUP', 'MONITOR', 'TROUBLESHOOT', 'Save', 'Reset', 'Actions', and 'Admin'. Below this is a secondary bar with 'M500Li', 'IP NETWORK', 'SIGNALING & MEDIA', and 'ADMINISTRATION'. The left sidebar shows a tree view with 'TOPOLOGY VIEW' expanded, containing 'CORE ENTITIES', 'CODERS & PROFILES', and 'GATEWAY'. Under 'GATEWAY', 'Trunks & Groups' is selected, and 'Trunk Groups' is highlighted. The main area displays the 'Trunk Group Table' with a 'Disable' dropdown and a '1-12' range selector. The table has columns: GROUP INDEX, MODULE, FROM TRUNK, TO TRUNK, CHANNELS, PHONE NUMBER, TRUNK GROUP ID, and TEL PROFILE NAME. Two rows are highlighted with a red border: Row 1 (Index 1, Module 2 FXS, Channels 1, Phone Number 70111, Trunk Group ID 1, Tel Profile Name TelProfile_1) and Row 2 (Index 2, Module 2 FXS, Channels 2, Phone Number 70112, Trunk Group ID 1, Tel Profile Name TelProfile_1). Below the table are 'Register' and 'Un-Register' buttons, and at the bottom, 'Cancel' and 'APPLY' buttons.

GROUP INDEX	MODULE	FROM TRUNK	TO TRUNK	CHANNELS	PHONE NUMBER	TRUNK GROUP ID	TEL PROFILE NAME
1	Module 2 FXS			1	70111	1	TelProfile_1
2	Module 2 FXS			2	70112	1	TelProfile_1
3							None
4							None
5							None
6							None
7							None
8							None
9							None
10							None
11							None
12							None

8.10.2. Trunk Group Settings

Click on **SETUP** in the title bar. Select **Signaling & Media** in the toolbar. Select **Gateway → Trunks & Groups → Trunk Group Settings** in the left pane. Click **Edit** (not shown)

- Input **1** for the **Trunk Group ID**
- Select **By Dest Phone Number** for **Channel Select Mode**
- Select **Per Endpoint** for **Registration Mode**
- Enter **avaya.com** for the Gateway
- Select **#0 [Default_IPG]** for the **Serving IP Group**

Click **APPLY**.

The screenshot displays the Avaya Aura Management GUI. The top navigation bar includes tabs for SETUP, MONITOR, TROUBLESHOOT, and a highlighted Save button. Below this, the left sidebar shows a tree view with categories like CORE, CODE, GATEWAY, and SIP. The main content area is titled 'Trunk Group Settings' and is divided into two panels: GENERAL and SIP CONFIGURATION. The GENERAL panel contains fields for Index (0), Name, Trunk Group ID (1), Channel Select Mode (By Dest Phone Number), Registration Mode (Per Endpoint), and Used By Routing Server (Not Used). The SIP CONFIGURATION panel contains fields for Gateway Name (avaya.com), Contact User, Serving IP Group (#0 [Default_IPG]), and MWI Interrogation Type. The Save button in the top toolbar and the APPLY button at the bottom of the form are both highlighted with red boxes. The STATUS section at the bottom right shows Admin State as Unlocked.

8.10.3. Tel-to-IP Routing

Click on **SETUP** in the title bar. Select **Signaling & Media** in the toolbar. Select **Gateway → Routing → Tel-to-IP Routing** in the left pane. Click **Edit** (not shown)

- Enter an appropriate value for **Name**
- Input **1** for the **Source Trunk Group ID**
- Select **#0 [SIPInterface_0]** for the **SIP Interface**
- If the Mediant 500Li is located within the enterprise, input Session Manager IP address used in **Section 5.4** for **Destination IP Address** e.g., **10.64.110.212** (not shown)
- If the Mediant 500Li is located in a remote location, input the SBCE external interface B1 IP address used by remote workers in **Section 7.2** for **Destination IP Address** e.g., **10.64.102.243**
- Input **5061** for the **Destination Port**
- Select **TLS** for the **Transport type**

Click **APPLY**.

Note: Tel-IP-Routing is set up to use the destination address. Mediant 500Li can be configured to use the default proxy which negates the need for the Tel-to-IP Routing configuration. Refer to **reference [4]** for more information

The screenshot shows the Audiocodes Mediant 500Li configuration interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The left sidebar shows a tree view with 'GATEWAY' expanded, and 'Tel-to-IP Routing' selected. The main configuration area is titled 'Tel-to-IP Routing [To Session Manager]'. It contains several sections: 'GENERAL' with fields for 'Index' (0), 'Name' ('To Session Manager'), and 'Connectivity Status' (Not Available); 'MATCH' with fields for 'Source Trunk Group ID' (1), 'Source Phone Pattern' (*), 'Source Tag', 'Destination Phone Pattern' (*), and 'Destination Tag'; 'ACTION' with fields for 'Destination IP Group' (..), 'SIP Interface' (#0 [SIPInterface_0]), 'Destination IP Address' (10.64.102.243), 'IP Profile' (..), 'Destination Port' (5061), and 'Transport Type' (TLS); and 'ADVANCED' with fields for 'Call Setup Rules Set ID' (-1), 'Forking Group' (-1), and 'Cost Group' (..). The 'Save' button is highlighted in the top bar. The bottom of the screen shows a summary of the configuration: 'Source Trunk Group ID: 1' and 'Destination Port: 5061'.

8.10.4. IP-to-Tel Routing

Click on **SETUP** in the title bar. Select **Signaling & Media** in the toolbar. Select **Gateway → Routing → IP-to-Tel Routing** in the left pane. Click **Edit** (not shown)

- Enter an appropriate value for **Name** e.g., **Session Manager to Tel**
- Select **#0 [SIPInterface_0]** for the **Source SIP Interface**
- Select **1** for the **Trunk Group ID**

Click **Apply**.

The screenshot shows the Audiocodes M500LI configuration interface. The top navigation bar includes 'SETUP', 'MONITOR', 'TROUBLESHOOT', 'Save', 'Reset', 'Actions', and 'Admin'. The left sidebar shows a tree view with 'IP NETWORK', 'SIGNALING & MEDIA', and 'ADMINISTRATION'. The main window displays the 'IP-to-Tel Routing [Session Manager to Tel]' configuration form. The form is divided into two main sections: 'GENERAL' and 'ACTION'.

GENERAL Section:

- Index:** 0
- Name:** Session Manager to Tel
- MATCH Section:**
 - Source SIP Interface:** #0 [SIPInterface_0]
 - Source IP Address:** *
 - Source Phone Pattern:** *
 - Source Host Pattern:** *
 - Source Tag:**
 - Destination Phone Pattern:** *
 - Destination Host Pattern:** *
 - Destination Tag:**

ACTION Section:

- Destination Type:** Trunk Group
- Trunk Group ID:** 1
- Source IP Group:** --
- IP Profile:** --
- Trunk ID:** -1
- Call Setup Rules Set ID:** -1

At the bottom of the form, there are 'Cancel' and 'APPLY' buttons. Below the form, there is a summary table:

Field	Value
Source Phone P...	*
Source Host Pa...	*
Source Tag	
Call Setup Rule...	-1

8.10.5. Authentication

Click on **SETUP** in the title bar. Select **Signaling & Media** in the toolbar. Select **Gateway** → **Analog Gateway** → **Authentication** in the left pane. Select the first entry created from **Section 8.10.1**. Click **Edit** (not shown)

- Input the SIP user created in **Section 6.8** above for **User Name**
- Input the analogous SIP user password for **Password**

Click **APPLY**.

Repeat administration for the second extension.

The screenshot shows the Audiocodes MD500Li Authentication configuration window. The window has a dark blue header with the Audiocodes logo and navigation tabs: SETUP, MONITOR, TROUBLESHOOT, Save, Reset, Actions, and Admin. The left sidebar shows a tree view with 'GAT' selected. The main area is divided into two tabs: 'GENERAL' and 'CREDENTIALS'. The 'GENERAL' tab contains fields for Index (0), Module (2), Port (1), and Port Type (FXS). The 'CREDENTIALS' tab contains fields for User Name (70111) and Password (a masked field). A red box highlights the 'CREDENTIALS' tab and its fields. At the bottom of the window are 'Cancel' and 'APPLY' buttons.

8.10.6. Gateway General Settings

Click on **SETUP** in the title bar. Select **Signaling & Media** in the toolbar. Select **Gateway** → **Gateway General Settings** in the left pane.

- Select **G.711 Transport** for the **Fax Signaling Method**
Click **APPLY**.

The screenshot shows the Audiocodes M500Li configuration interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The left sidebar shows the 'GATEWAY' section expanded, with 'Gateway General Settings' selected. The main content area is titled 'Gateway General Settings' and is divided into two tabs: 'FAX' and 'BEHAVIOR'. Under the 'FAX' tab, the 'Fax Signaling Method' is set to 'G.711 Transport' (highlighted with a red box). Other settings under 'FAX' include 'Detect Fax on Answer Tone' (Initiate T.38 on Prean), 'SIP T.38 Version' (Not Configured), 'T.38 Fax Session' (Disable), and 'T.38 Fax Max Buffer' (3000). Under the 'BEHAVIOR' tab, settings include 'NAT IP Address' (::), 'Channel Select Mode' (Cyclic Ascending), 'Tel to IP No Answer Timeout' (180), 'Play Ringback Tone to IP' (Don't Play), 'Play Ringback Tone to Tel' (Prefer IP), 'Progress Indicator to IP' (Not Configured), 'Enable Semi-Attended Transfer' (Disable), 'Forking Handling Mode' (Parallel handling), and 'Enable Comfort Tone' (Disable). At the bottom right, there are 'Cancel' and 'APPLY' buttons.

8.10.7. Supplementary Services Settings

Click on **SETUP** in the title bar. Select **Signaling & Media** in the toolbar. Select **Gateway → DTMF & Supplementary → Supplementary Services Settings** in the left pane.

- Select **Enable** for **Enable MWI**
- Select **Yes** for **Subscribe to MWI**
- If the Mediant 500Li is located within the enterprise, input Session Manager IP address used in **Section 5.4** for **MWI Server IP Address** e.g., **10.64.110.212** (not shown)
- If the Mediant 500Li is located in a remote location, input the SBCE external interface B1 IP address used by remote workers in **Section 7.2** for **MWI Server IP Address** e.g., **10.64.102.243**

Click **APPLY**.

The screenshot shows the Audiocodes M500Li web interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The left sidebar shows the navigation tree with 'Supplementary Services Settings' selected. The main content area is titled 'Supplementary Services Settings' and contains two tabs: 'GENERAL' and 'TRANSFER'. The 'GENERAL' tab is active, showing settings for 'Enable Caller ID', 'Answer Supervision', 'Flash Keys Sequence Style', 'Flash Keys Sequence Timeout', 'Enable NRT Subscription', 'NRT Subscribe Retry Time', 'Generate Metering Tones', 'AoC Support', 'Reminder Ring', and 'Line Transfer Mode'. The 'TRANSFER' tab is also visible, showing settings for 'Enable Transfer', 'Transfer Prefix', and 'Blind Transfer'. A 'MESSAGE WAITING INDICATOR' section is highlighted with a red box, containing 'Enable MWI' (set to 'Enable'), 'Subscribe to MWI' (set to 'Yes'), and 'MWI Server IP Address' (set to '10.64.102.243'). At the bottom of the page, there are 'Cancel' and 'APPLY' buttons.

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, SBCE, and Mediant 500Li.

9.1. Avaya Aura® Communication Manager and Avaya Aura® Session Manager

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 5.6.1**. The **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 successful registration from AudioCodes Mediant 500Li to Session Manager via the System Manager console. Navigate to **Home → Session Manager → System Status → User Registration**. The SIP users administered in **Section 6.8** should appear. When Mediant 500Li is located in the enterprise, the IP Address should be that of Mediant 500Li administered in **Section 8.1.1**.

AVAYA Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 admin

Home Session Manager

User Registrations

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

View ▾ Default Export Force Unregister **AST Device Notifications:** Reboot Reload ▾ Failback As of 12:43 PM Advanced Search

43 Items Show 15 ▾ Filter: Enable

	Details	Address ▾	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered			
											Prim	Sec	Surv	Visiting
<input type="checkbox"/>	► Show	70112@avaya.com	User 2	AudioCodes	DevConnect	10.64.10.82	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	70111@avaya.com	User 1	AudioCodes	DevConnect	10.64.10.82	<input type="checkbox"/>	<input type="checkbox"/>	1/10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	70104@avaya.com	SIP	Station 4	---	192.168.5.3	<input type="checkbox"/>	<input type="checkbox"/>	1/3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	70103@avaya.com	SIP	Station 3	---	192.168.4.140	<input type="checkbox"/>	<input type="checkbox"/>	1/10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	70102@avaya.com	SIP	Station 2	DevConnect	10.64.10.201	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	70101@avaya.com	SIP	Station 1	---	192.168.5.2	<input type="checkbox"/>	<input type="checkbox"/>	1/2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	Juan	71555	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	S2415	VTech	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	SIP	Station 8	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	S2415	VTech	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

When Mediant 500Li is configured as Remote Worker, the IP address should be that of the internal Remote Worker interface IP shown in **Section 7.5**, e.g., **10.64.110.243**. The **Remote Office** column will be checked (representative image below if Session Manager Remote Access is configured). See **Reference [2]** in **Section 11** for administration details.

Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered	Prim	Sec	Surv	Visiting
Show	70111@avaya.com	User 1	AudioCodes	DevConnect	10.64.110.243	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Show	70112@avaya.com	User 2	AudioCodes	DevConnect	10.64.110.243	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Show	70115@avaya.com	J159	SIP Station	DevConnect	10.64.10.203	<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"/>	<input type="checkbox"/>
Show	70102@avaya.com	SIP	Station 2	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"/>	<input type="checkbox"/>
Show	---	Juan	71555	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

9.2. Avaya Session Border Controller for Enterprise

On SBCE, navigate to **Status** → **User Registrations**. Mediant 500Li SIP users should display as registered to Session Manager.

AOR	SIP Instance	SBC Device	SM Address	Registration State
70111@avaya.com	---	SBCE812	10.64.110.212(NONE)	REGISTERED
70112@avaya.com	---	SBCE812	10.64.110.212(NONE)	REGISTERED

9.3. AudioCodes Mediant 500Li

Click on **MONITOR** in the title bar. Select **MONITOR** in the toolbar. Select **VOIP STATUS** → **Proxy Sets Status** in the left pane.

- If the Mediant 500Li is located within the enterprise, verify the **ADDRESS** is Session Manager's IP address configured in **Section 5.4** (not shown). Verify the **STATUS** is **ONLINE**.
- If the Mediant 500Li is located in a remote location, verify the **ADDRESS** is the SBCE external interface B1 IP address used by remote workers from **Section 7.2**. Verify the **STATUS** is **ONLINE**.

The screenshot displays the AudioCodes Mediant 500Li Monitor interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The 'MONITOR' tab is active. Below the navigation bar, there's a search bar with the placeholder text 'Entity, parameter, value'. The main content area is divided into a left sidebar and a main panel. The sidebar has a 'MONITOR' section with a 'SUMMARY' link. Under 'VOIP STATUS', 'Proxy Sets Status' is highlighted. The main panel shows the 'Proxy Sets Status' table, which updates every 60 seconds. The table has columns for PROXY SET ID, NAME, MODE, KEEP ALIVE, ADDRESS, PRIORITY, WEIGHT, SUCCESS COUNT, FAILURE COUNT, and STATUS. A single row is visible with the following data: PROXY SET ID 0, NAME ProxySet_0, MODE Parking, KEEP ALIVE Enabled, ADDRESS 10.64.102.243:5061(*), PRIORITY -, WEIGHT -, SUCCESS COUNT 4525, FAILURE COUNT 82, and STATUS ONLINE. The ADDRESS and STATUS cells are highlighted with a red border.

PROXY SET ID	NAME	MODE	KEEP ALIVE	ADDRESS	PRIORITY	WEIGHT	SUCCESS COUNT	FAILURE COUNT	STATUS
0	ProxySet_0	Parking	Enabled	10.64.102.243:5061(*)	-	-	4525	82	ONLINE

Click on **MONITOR** in the title bar. Select **MONITOR** in the toolbar. Select **VOIP STATUS** → **Registration Status** in the left pane. Verify the configured FXS lines from **Section 8.10.1** are registered.

The screenshot shows the Audiocodes M500Li MONITOR interface. The left sidebar contains the following menu items:

- MONITOR
 - SUMMARY
 - Device Information
 - Active Alarms
 - Alarms History
 - Activity Log
 - PERFORMANCE MONITORING
 - Performance Profile (0)
 - VOIP STATUS
 - IP-to-Tel Calls Count
 - Tel-to-IP Calls Count
 - Proxy Sets Status
 - Registration Status**
 - IP Connectivity
 - Gateway CDR History
 - NETWORK STATUS
 - DATA STATUS

The main content area displays the 'Registration Status' page. It includes the following sections:

- Registration Status**
 - Registered Per Gateway: NO
 - Ports Registration Status

GATEWAY PORT	STATUS
Module 2 Port 1 FXS	REGISTERED
Module 2 Port 2 FXS	REGISTERED
Module 2 Port 3 FXS	NOT REGISTERED
Module 2 Port 4 FXS	NOT REGISTERED
Module 3 Port 1 FXS	NOT REGISTERED
Module 3 Port 2 FXS	NOT REGISTERED
Module 3 Port 3 FXS	NOT REGISTERED
Module 3 Port 4 FXS	NOT REGISTERED
- Accounts Registration Status**

INDEX	GROUP TYPE	GROUP NAME	STATUS
-------	------------	------------	--------
- Phone Numbers Status**

PHONE NUMBER	GATEWAY PORT	STATUS
--------------	--------------	--------

Make calls to and from the analog lines to Avaya endpoints located in the enterprise and verify two-way audio path.

10. Conclusion

These Application Notes describe the configuration steps required for AudioCodes Mediant 500Li to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager in the enterprise configuration or a remote worker configuration employing Avaya Session Border Controller for Enterprise. All feature and serviceability test cases completed and pass with observations/exceptions noted in **Section 2.2**

11. Additional References

This section references the product documentation relevant for these Application Notes.

- [1] *Administering Avaya Aura® Communication Manager*, Issue 12, Release 8.1.x, July 2021
- [2] *Administering Avaya Aura® Session Manager*, Issue 10, Release 8.1.x, September 2021
- [3] *Administering Avaya Session Border Controller for Enterprise*, Issue 5, Release 8.1.x, August 2021
- [4] *AudioCodes Mediant 500Li MSBR Users Manual*, Version 7.2, March 18, 2021:
- [5] *AudioCodes Mediant 500Li MSBR CLI Reference Guide*
- [6] *AudioCodes Mediant 500Li Security Setup CLI Configuration Guide*

AudioCodes Mediant 500Li General references:

<https://www.audiocodes.com/library/technical-documents?productFamilyGroup=1647&productGroup=27483&versionGroup=Version+7.2>

©2021 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.